

AFRL-IF-RS-TR-2002-109
Final Technical Report
May 2002



JOINT BATTLESPACE INFOSPHERE DISTRIBUTED TESTBED (JBI-DT)

Northrop Grumman Information Technology

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

**AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK**

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2002-109 has been reviewed and is approved for publication.

APPROVED: 

CHARLES E. FLYNN
Project Engineer

FOR THE DIRECTOR: 

RICHARD C. METZGER, Technical Advisor
Information Systems Demonstration & Integration
Information Directorate

REPORT DOCUMENTATION PAGE			<i>Form Approved</i> OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE May 2002	3. REPORT TYPE AND DATES COVERED Final Jan 01 – Oct 01	
4. TITLE AND SUBTITLE JOINT BATTLESPACE INFOSPHERE DISTRIBUTED TESTBED (JBI-DT)			5. FUNDING NUMBERS C - F30602-00-D-0159/0003 PE - 63789F PR - JBIT TA - PR WU - 03	
6. AUTHOR(S) Robert Edward Gann				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Northrop Grumman Information Technology Defense Mission Systems, Incorporated 12005 Sunrise Valley Drive, M/S G402 Reston Virginia 20191			8. PERFORMING ORGANIZATION REPORT NUMBER 02-053-0074	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Air Force Research Laboratory/IFSE 525 Brooks Road Rome New York 13441-4505			10. SPONSORING / MONITORING AGENCY REPORT NUMBER AFRL-IF-RS-TR-2002-109	
11. SUPPLEMENTARY NOTES AFRL Project Engineer: Charles E. Flynn/IFSE/(315) 330-4862/Charles.Flynn@rl.af.mil				
12a. DISTRIBUTION / AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.				12b. DISTRIBUTION CODE
13. ABSTRACT (Maximum 200 Words) This report discusses the development of Joint Battlespace Infosphere (JBI) Experimental Portal (JXP). The JXP is a role-based portal whose primary objective is to integrate legacy and emerging Command and Control, Intelligence, Surveillance and Reconnaissance (C2ISR) applications side-by-side in an Air Operations Center (AOC) workplace. This report describes the development of the JXP from the initial setup of the hardware through the initial operating capability (IOC). A detailed description of the JXP's role-based design is provided. Some of the challenges overcome during development are discussed.				
14. SUBJECT TERMS Joint Battlespace Infosphere, Portal, Web Based Access, Air Operations Center, Role Based Access, Oracle 9, Internet Application server, Web Based Desktop				15. NUMBER OF PAGES 93
				16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL	

Table of Content

1. Introduction	1
1.1 Identification	1
1.2 JBI-DT Overview	1
1.3 TO-03 Overview.....	1
1.4 Report Organization	2
2. Hardware Setup	3
3. Initial Software Build	4
4.0 Portal Development	5
4.1 Initial Portal Development	5
4.2 Design.....	8
4.3 Upgrading Portal Software	11
4.4 Building A Second Portal	12
4.5 Using Government PKI Certificates	13
4.5.1 Obtaining the PKI Certificates	13
4.5.2 Installing the Certificate	14
4.5.3 HTTPS and Redirection	14
4.6 Portlets.....	14
4.6.1 URL Services.....	15
4.6.2 Customer Feedback Portlet.....	16
4.7 Securing JXP	16
5. Configuration Management	20
6. SIPRNET Migration	22
7. Oracle 9i Beta Program	23
8. Conclusion	24
Appendix A – Oracle Technical Assistance Request Number 1939945.999	27
Appendix B. JBIX4 Screen Shots	40
Appendix C Chronology of Accomplishments Under TO-03 of JBI-DT Contract	77
Appendix D. Acronyms	83
Appendix E Oracle 9i Press Release	86

LIST OF FIGURES

	<u>Page</u>
Figure 1 Oracle Portal Home Page	5
Figure 2 Edit HTML Portlet Screen.....	6
Figure 3 Weather Channel HTML Portlet	6
Figure 4 Oracle Application Components	6
Figure 5 Content Area Items.....	7
Figure 6 JXP Roles	8
Figure 7 Air Operations Center.....	9
Figure 8 Commander Air Force Forces	9
Figure 9 MCP Tab Selected.....	10
Figure 10 Master Caution Panel	11
Figure 11 Self-Registration Portlet.....	12
Figure 12 ATO/ACO Web Browser Image	13
Figure 13 IGN.COM Being Pushed Through JBIX4.....	15
Figure 14 Customer Feedback Page	16
Figure 15 Public User's View of the Role Portlet.....	17
Figure 16 JBIADMIN's View of the Role Portlet.....	17
Figure 17 Portal30's View of the Role Portlet	18
Figure 18 Public User's View of Page	18
Figure 19 Authenticated User's View of Page	19
Figure 20 Portal Home Page with Timing Enabled	21
Figure B-1 JBIX4 Home Page	40
Figure B-2 Air Operations Center.....	41
Figure B-3 Commander, Air Force Forces	42
Figure B-4 Foreign Disclosure Officer	43
Figure B-5 Strategy Division	44
Figure B-6 GAT Team Chief.....	45
Figure B-7 Targeteers/Weaponers	46
Figure B-8 Information Warfare Analysts.....	47
Figure B-9 Combat Plans Division	48
Figure B-10 Strike Planner	49
Figure B-11 MAAP Team Chief.....	50
Figure B-12 C2 Planning Team Chief	51
Figure B-13 Tanker Planner.....	52
Figure B-14 Combat Operations Division	53
Figure B-15 Weather Support Team.....	54
Figure B-16 Tanker Duty Officer	55
Figure B-17 Senior Offensive Duty Officer	56
Figure B-18 ABC2DO	57
Figure B-19 Senior Air Defense Officer.....	58
Figure B-20 Theater Missile Defense Officer	59
Figure B-21 Interface Control Officer	60

Figure B-22 Intelligence, Surveillance and Reconnaissance Division	61
Figure B-23 Chief of Targets	62
Figure B-24 Chief of Collections Operations	63
Figure B-25 Air Mobility Division	64
Figure B-26 Specialty Functions	65
Figure B-27 Communications Support	66
Figure B-28 Information Management Staff	67
Figure B-29 AOC IM System Operator	68
Figure B-30 Data Base Administrator	69
Figure B-31 System Administrator	70
Figure B-32 Portal Administrator	71
Figure B-33 Information System Security Manager	72
Figure B-34 C2ISR Applications	73
Figure B-35 Programs and Briefings	74
Figure B-36 Links	75
Figure B-37 What's New	76

LIST OF TABLES

Table 1 Unix Partition Layout	4
Table 2 Commander, Air Force Forces Applications	11

1. Introduction

1.1 Identification

This final report documents the work performed and lessons learned under Task Order (TO-03) of the Joint Battlespace Infosphere (JBI) – Distributed Testbed (DT) contract.

1.2 JBI-DT Overview

In Chapter 9 of the “USAF Scientific Advisory Report on Building the Joint Battlespace Infosphere”, two recommendations were made. The first recommendation was “to create a JBI Testbed now for JEFX-00 participation”. The second recommendation was to link the JBI Testbed to other services in Digitized Battlefield and Network Centric Warfare”. In response the JBI-DT contract was established. The JBI-DT contract is a \$24.9M, 5-year, IDIQ for AFRL that began on 25 Jul 00. The JBI-DT program is scoped to establish a multi-site (AFRL, ESC (CUBE), Langley (OSC), Hurlburt (C2B), Nellis (DBCC/TCTC), USJFCOM (JBC)) distributed testbed to acquire, test/evaluate, and recommend implementation of JBI-technology initiatives into the USAF C4I systems baseline. The contract scope includes managing a spiral development plan for AF-wide evolution of JBI-based systems as well as all operations of the DT including coordinating with all possible sources of JBI initiatives within the DoD, Academia, and industry.

TO-03 under the JBI-DT contract was to establish, operate, and maintain a web portal at the Command and Control Technology Center (C2TC) located at Rome, NY. The period of performance was from 16 January 01 to 31 October 01.

1.3 TO-03 Overview

Part of the JBI vision is to link legacy Command and Control (C2) resources together. In pursuit of this vision TO-03 was established to install and evaluate Oracle’s 9i Internet Application Server (IAS). A key component of IAS is Oracle Portal which provides a secure, manageable environment with a scalable architecture. It also provides a framework that can be extended across multiple sites and domains. The objective of the TO was to establish a JBI Experimental Portal (JXP) that integrated legacy and emerging Command and Control, Intelligence, Surveillance and Reconnaissance (C2ISR) applications side-by-side in an Air Operations Center (AOC) workplace.

The goals established for the JXP are listed below. These goals were obtained from a briefing called “Joint Battlespace Infosphere Experimental Portal” (JXP) dated 13 July 2001 by Mr. Charles Flynn. The status of these goals will be addressed at the conclusion of this report.

JXP Goals

- Build Role-Based Portal for C2ISR Users
- Use Commercial Off The Shelf (COTS) Netscape or Explorer browser
- Work through USAF Firewalls on HTTP (HTTPS) Protocol
- Use USAF-Licensed COTS: Oracle 9iAS and Oracle 8i & 9i
- Impose no additional burden to System Administrators
- Require no new hardware or software in Operations Cells
- Integrate and Demonstrate Research and Development (R&D) Applications with SOR
- Enable users to logon to Portal from any network workstation
- Provide centralized Database Administration (DBA) and Portal Administration on Server

1.4 Report Organization

This report details the technical work performed under TO-03 of the JBI-DT contract. Technical challenges encountered and solutions are presented throughout the report. Numerous screen shots from the portal are included. The report is structured as follows:

- Section 2 describes the hardware used on this project.
- Section 3 discusses the software used to build the portals.
- Section 4 details the portal development. The section begins by presenting some of the simple early development challenges. Next the portal's role-based design is described. Following the design discussion is a presentation of the challenges encountered in upgrading the portal software, implementing a second portal, and incorporating the use of Public Key Infrastructure (PKI) certificates. This section is concluded with sections on portlets and securing the portal.
- Section 5 briefly describes the configuration management (CM) practices used to support the hardware and software.
- Section 6 takes a look ahead to migrating the portal to the Secret Internet Protocol Router Network (SIPRNET).
- Section 7 discusses RRS' participation in the Oracle 9i Beta Program.
- Section 8 presents the concluding remarks and reexamines the JXP goals.
- Appendix A contains the text from a Technical Assistance Request (TAR) to Oracle.

- Appendix B presents a set of screen shots from jbix4.
- Appendix C provides a brief chronology of the accomplishments on TO-03.
- Appendix D presents a list of acronyms.
- Appendix E contains the press release on the Oracle 9i Beta Program.

2. Hardware Setup

SOW 4.1.3 Configure and integrate Government Furnished IT equipment into the JBI-DT in the Command and Control Technology Center (C2TC) and Systems Concepts & Applications Testbed (SCAT) Laboratory at RRS.

The Government furnished four machines to be used for portal development and deployment. The four machines consisted of two Enterprise 3500s by Sun (hostnames jbix0 and jbix3) and two ProReliant 8500s by Compaq (hostnames jbix1 and jbix4). The Government specified that they be installed in the C2TC. The original plan provided for one Compaq and one Sun being used for the Unclassified portal and one Compaq and Sun being used for the Secret Internet Protocol Router Network (SIPRNET) portal. In each case, the Compaq was going to be used for development and the Sun for deployment.

The basic hardware configuration is listed below:

Sun Enterprise 3500 – Dual UltraSparc 300 MHz processors, 1GB RAM, 2 20GB removable hard disks

Compaq ProReliant 8500 – Dual Xenon 700 MHz processors, 1GB RAM, 2 9GB Internal hard disks, 4 18GB removable hard disks

3. Initial Software Build

SOW 4.1.1 Implement the Information Technology (IT) systems in the JBI-DT. Utilize daily operations to define and document the changes necessary to USAF IT.

SOW 4.1.2 Plan the integration of GOTS/COTS components into the JBI-DT.

Solaris 7 was originally installed on jbix0 and jbix3. The servers were partitioned as follows:

Disk 0

Partition	Slice	Space Allocation
/	0	2048MB
swap	1	1024MB
/var	3	1024MB
/export/home	4	1024MB
/usr	5	2560MB
/vendor1	6	9580MB

Disk 1

Partition	Slice	Space Allocation
/vendor2	4	8630MB
/vendor3	5	8639MB

Table 1 Unix Partition Layout

Windows 2000-Advanced Server was installed on jbix1 and jbix4. The internal drives were RAID-5 striped yielding about 9GB of usable disk space. The 4 18GB removable drives were also RAID-5 striped providing about 53GB of usable disk space.

Oracle 8.1.7 was loaded on all of the servers IAS 1.0.2.1. Portal 3.0.6.6.5 was part of this release. However, the Government decided to participate in the Oracle 9i beta program and jbix0 was used for this purpose. Consequently, Solaris 8 and Oracle 9i was installed on jbix0. The same partitioning scheme was used.

After the operating system was loaded, the RL/IFOS Security checklist was used to secure the workstation. Once secured, the January 2001 Sun patch cluster was applied. The patch cluster included a broken rmmount binary that prevented removable media from being mounted upon insertion. Once the problem was

identified, several patches were backed out and the problem was rectified. Subsequent patch clusters were applied without issue.

4.0 Portal Development

SOW 4.1.1 Implement the Information Technology (IT) systems in the JBI-DT. Utilize daily operations to define and document the changes necessary to USAF IT.

4.1 Initial Portal Development

Initial development was slow. Oracle Portal is a comprehensive program with many features and options. It took time to learn to effectively navigate through the menus.



Figure 1 Oracle Portal Home Page

Initially, the development focused on simply displaying links on a page. Substantial time was spent using the HTML portlet provided by Oracle. A portlet is a region that can display data. The HTML portlet allows the user to enter any HTML in a portlet and then display it on a page.



Figure 2 Edit HTML Portlet Screen

This approach had two problems. First, the portlet was page specific and not reusable. One of the powers of portlets is their reusability. Once a portlet is developed and published to the portal, it can then be reused. The second issue pertained to a customize link that which appeared in the portlet banner. This link was not removable in version 3.0.6.6.5 of portal and it exposed designer areas of the portal that shouldn't be displayed to the public.



Figure 3 Weather Channel HTML Portlet

The problem was later resolved by using the dynamic application component, one of several application components provided by Oracle to support development.



Figure 4 Oracle Application Components

Oracle does provide a portlet development kit (PDK) that allows the developer to control every aspect of development, including the removal of the customize link.

However, it is time consuming to build the individual elements that make up a portlet. Sometimes the developer is forced to decide between flexibility and shorter development times.

Another early development issue was how to load images into the portal and then display them via a uniform resource locator (URL). During traditional web development, images are usually stored in directory under the document root and accessed directly via the tag. Oracle provides content areas for storing images. A content area is collection of information stored in the database. Many different types of items can be stored in a content area.

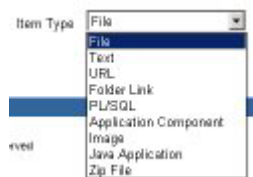


Figure 5 Content Area Items

Once an image was in the database, the next issue was determining the image's URL. Since the image is stored in the database, the URL is different. The URL to access the portal on jbix4 is <https://jbix4.dise.rl.af.mil/jxphome>, whereas the actual URL is <https://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome>.

The REDIRECT directive is used in the httpd.conf file to shorten the URL the user must type to access the portal. In the actual URL, "pls" represents the Apache module used to access the page. PORTAL30 is the database access descriptor (DAD) used to access the Oracle database. /url/page/jxphome is the document root relative path to the page. To determine the URL of an image in a content area, the same methodology was tried. That is, to access a particular image, the URL would be as follows:
<https://jbix4.dise.rl.af.mil/pls/portal30/FOLDER/FOLDERNAME/IMAGENAME>
where /FOLDER is the Oracle location of the content areas. /FOLDERNAME is the name assigned by a user to a folder (i.e. for instance images). IMAGENAME is the name assigned by a user to a particular image. However, it was discovered that the individual items, in this case images, were not named. The URL was eventually obtained by right clicking on the image, selecting properties, and then copying the URL from the window.

4.2 Design

SOW 4.1.7 Support the JBI Team Research and Development plans through participation with Government and industry partners in the spiral development of the JBI-DT.

SOW 4.1.9 Integrate existing USAF C2ISR systems with experimental systems in the JBI-DT. Existing USAF systems will include, but not be limited to GCCS-AF, TBMCS, SBMCS, DCGS, C2IPS, wfJBI, and Intelligence Data Handling Systems. The Government will determine the physical locations of systems within JBI-DT.

SOW 4.1.12 Coordinate the use of experimental software in operational Government networks. Integrate experimental software only after receiving permission from Government-identified National-level network authorities.

As was previously stated, the objective of TO-03 was to construct a portal that integrated legacy and newly developed Command and Control, Intelligence, Surveillance and Reconnaissance (C2ISR) applications side-by-side in an Air Operations Center (AOC) workplace. Section 2.5 of Air Force Instruction (AFI) 13-1AOC Volume 3 dated 6 MARCH 2000 divided the AOC into five divisions: Strategy; Combat Plans; Combat Operations; Intelligence, Surveillance, and Reconnaissance; and Air Mobility. Sections 9 and 10 of AFI 13-1 define the additional roles of Communications Support and Information Management Staff. In addition, RL/IFSE defined the Information Management Staff role.



Figure 6 JXP Roles

The AOC link provides access to the AOC page. From here, Commander Air Force Forces (COMAFFOR) can access all C2ISR applications. The COMAFFOR or CFACC link provides access to the Commander Air Force Forces page.



Figure 7 Air Operations Center

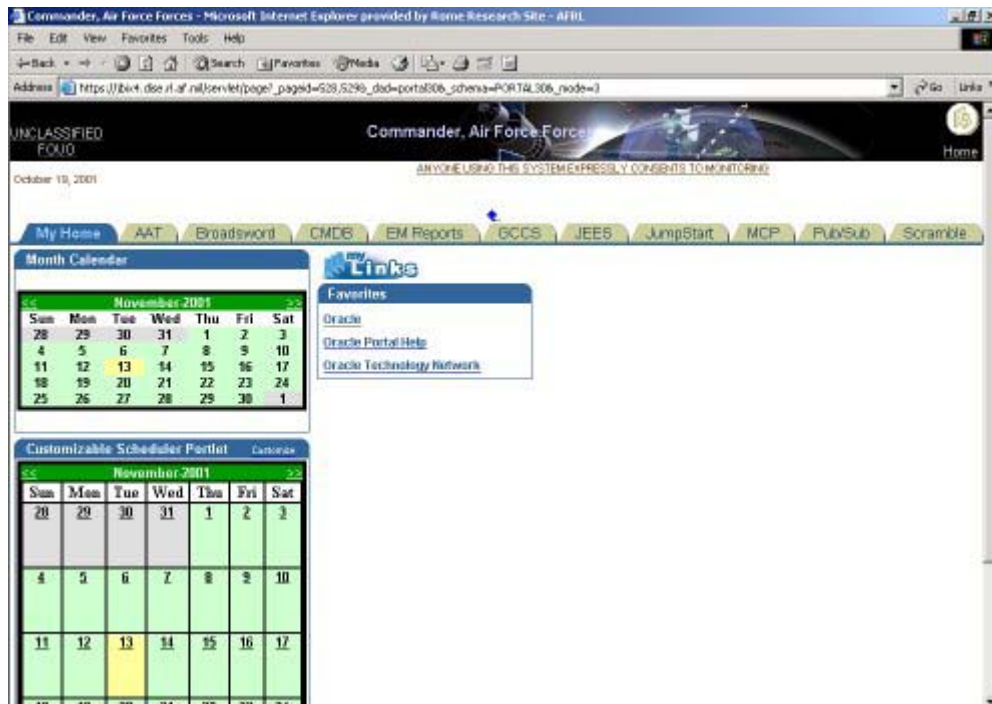


Figure 8 Commander Air Force Forces

Each of the tabs provides access to a C2ISR application. There is one additional tab, WebTAS (Web Enabled Timeline Analysis System), which provides access to the WebTAS homepage. As an example, if the Commander selects the MCP (Master Caution Panel) tab, he is taken to the MCP page. In the portlet window is a screen shot



Figure 9 MCP Tab Selected

from the MCP application. Each of the tabs has a corresponding screen shot for the particular application. The screen shot helps the user decide whether or not he has selected the right application. When the user selects the MCP image, he is taken to the actual application. The application is opened in a new window so the user can launch another instance of the same application, or a different application. The JXP is designed for users with large monitors and data walls. This allows the user to run multiple instances of the same application with different parameters or to run multiple applications at the same time. The table below briefly summarizes the purpose of each of the applications/tabs.

Tab	Description
ATO/ACO	Collection of tools to view ATO/ACO
Broadsword	System that manages distributed, heterogeneous data resources
CMAPI	A set of software components an intelligence application can use to access one of several packages for map data visualization
CMDB	AFRL's configuration management database
EM Reports	Series of templates that pulls data for AODB and stores it in report format
GCCS	Command and control system for joint and coalition forces
JEES	System that evaluates a weapon's system performance based on weather conditions
Jumpstart	Demonstration of a publication/subscription application using Oracle tools
MCP	Display that monitors the health of TBMCS-like connectivity and processes
PUB/SUB	Instrumented publication/subscription application running within the JBI 24x7 system

Scramble	System that sends a message to aircraft on Alert status to react to an immediate situation
WebTAS	Set of analytical tools allowing organizations to fuse, visualize, and interpret disparate sources of information, while remaining domain-tailorable to the user

Table 2 Commander, Air Force Forces Applications

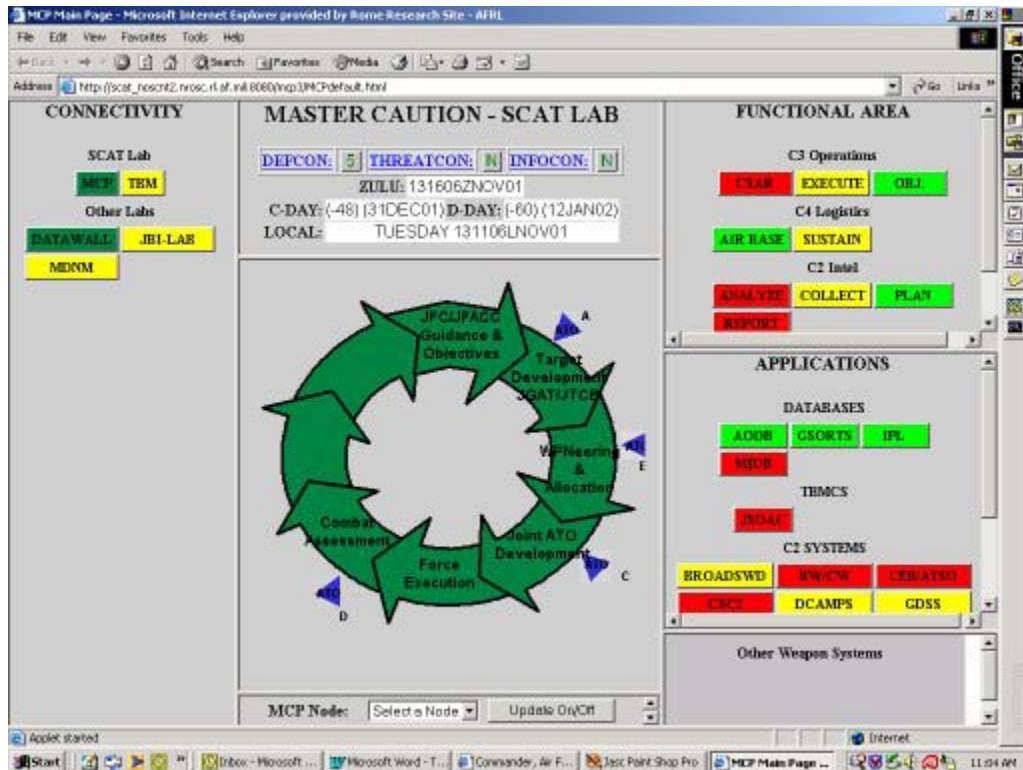


Figure 10 Master Caution Panel

4.3 Upgrading Portal Software

SOW 4.1.8 Provide recommendations on technology insertion into JBI-DT, identify necessary infrastructure improvements to support JBI spirals, and provide technical liaison with commercial vendors and suppliers to the JBI-DT.

A decision was reached to upgrade the Oracle Portal software from version 3.0.6.6.5 to 3.0.8.9.8. The newer version fixed many bugs and provided a self-registration feature where a JXP user could create his/her own portal account.



Figure 11 Self-Registration Portlet

When it was time to upgrade, it was discovered that there were no migration scripts available to migrate from version 3.0.6.6.5 to 3.0.8.9.8 without first migrating to version 3.0.7. Rather than performing the intermediate upgrade that would be very time consuming, it was decided to migrate straight to the newest version by manually updating the upgrade scripts and database tables. The upgrade failed and the existing portal became corrupted. As a result, a fresh install of version 3.0.8.9.8 was performed and the portal was rebuilt from the beginning.

4.4 Building A Second Portal

Once the portal was reestablished on version 3.0.8.9.8, a decision was made to build a mirror image on jbix4 (Windows 2000 Advanced Server). The method to get the content from jbix3 to jbix4 was to use Oracle's import/export scripts. Oracle Note: 133135.1 "Export/Import in Portal" detailed the steps involved to accomplish the task. The first step was to install Portal 3.0.8.9.8 on jbix4 because the scripts do not support different versions. The remainder of the steps pertained to exporting and importing the login server information, security information, applications, content areas, and pages.

After the exports and imports were complete, the portal on jbix4 did not work. First, most of the dynamic applications developed on jbix3 were changed during the migration. Dynamic applications have been primarily used to hold URLs. Remember that the dynamic applications do not allow the user to modify the portlet via the customize link. The DADS in the URL were changed from portal30 to the dynamic application owner. For example:

`http://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome/aoc`

was changed to

`http://jbix4.dise.rl.af.mil/pls/jbi/url/page/jxphome/aoc.`

The second problem was that Oracle had changed the image names during the migration. On jbix3, the images were given a three digit number as a name by Oracle once they were loaded into a content area. On jbix4, the images were assigned a different 4 digit number as a name. The image in the portlet below name was changed from 339.jpg on jbix3 to 3128.jpg on jbix4.



Figure 12 ATO/ACO Web Browser Image

The third problem pertained to the portlets. Several steps are required which are not specified in Oracle Note: 133135.1. First, numerous files had to be transferred from jbix3 to jbix4. Portlets consist of many files that are not loaded into the database. Second, the database schemas had to be exported and imported. Third, the portlet had to be reregistered. Registration establishes the means by which the portlets communicate with the portal. Portlets do not have to reside on the same machine as the portal.

Once these three problems were overcome, the portal on jbix4 became operational. As was discovered, the import/export process is somewhat complex and requires planning. The complexity arises from the fact that multiple schemas have to be exported from the database and all of the data does not reside in the database.

4.5 Using Government PKI Certificates

DoD has a requirement that all web portals must use Government Public Key Infrastructure (PKI) certificates. This involves two steps: obtaining the certificates and then installing them. Since jbix4 is tentatively scheduled for use on the RRS Intranet, it was the first host to get the certificates installed.

4.5.1 Obtaining the PKI Certificates

The first step was to obtain the document Requesting Web Server DoD Class 3 (Release 2) PKI Digital Certificates and Oracle Note: 136153.1 Configuring SSL for Portal. This document provides the necessary information to correctly generate a certificate request, explains how to install the DoD Root Certificate Chain in the browser, and tells where to submit the certificate request. Using the aforementioned documents, the next step is to generate the certificate request.

Once the certificates are generated, the DoD Root Certificate Chain must be installed in the browser. After the certificate chain is installed, the certificate request must be submitted to DISA. At the same time, a DoD PKI Server Certificate Requirement Form must be submitted to the Local Registration Authority, who at RRS is Hal Arsic. Usually after a couple of days, an email is sent with directions on where to get the certificate.

4.5.2 Installing the Certificate

Installing the certificates and configuring portal to use https is documented well in the Oracle note with the exception of creating the Secure Socket Layer (SSL) certificate chain file. When trying to access jbix4 using SSL, the following error was reported:

```
javax.net.ssl.SSLException: SSL handshake failed:  
X509CertChainIncompleteErr.
```

The error was due to a malformed certificate chain file. This error was not resolved until an Oracle bulletin prepared for Gunter AFB on setting up SSL on 9iAS was obtained that explained how to correctly construct the file.

4.5.3 HTTPS and Redirection

After SSL was configured on jbix4, the portal did not render page requests consistently. Upon login, logout, or anytime in between, the portal would not display the requested page and would instead yield the error message “No DAD configuration Found”. This error occurred often, but not consistently. Finally, it was determined that the error occurred every time an application was edited then canceled. At this point, a Technical Assistance Request (TAR) was opened with Oracle. After two weeks of working with Oracle, it was identified that the `wwv_redirect.url()` function does not handle https at all. This means that accessing any page or any application on the portal could fail. The problem was reported as Bug# 1714880 against Portal 3.0.8.9.8. The problem was rectified in version 3.0.9. Oracle issued patch # 1714880 for version 3.0.8.9.8. Once the patch was installed, jbix4 began rendering pages correctly.

4.6 Portlets

Portlets are regions that can display data. They can consist of URLs, Java, SQL statements and many other forms of data. With portlets, web content can be pushed from other sources and data can be fairly easily pulled from disparate database tables. Applications can be built with minimal knowledge of the portal infrastructure. Portlets are highly extensible. By utilizing the Portal Development Kit (PDK), many aspects portlet display behavior can be controlled. For example, if a portlet were built from scratch using the PDK, then the designer can control whether or not the customize link is displayed. The PDK is published

monthly and it has been installed several times on jbix3 and jbix4. The PDK consists of documentation on how to build portlets and it also provides sample portlets that can be used and modified. Many portlets from previous PDKs have been installed. Two portlets in particular that warrant discussion are the URL Services Portlet and the Customer Feedback Portlet.

4.6.1 URL Services

URL Services is part of the PDK that allow web content to be integrated into the portal. Any object that can be published such as a java applet or an html page can be pushed to the portal. For example the following page is from www.ign.com. The content is pushed to jbix4 and is displayed at <https://jbix4.dise.rl.af.mil/jxphome/ign>.

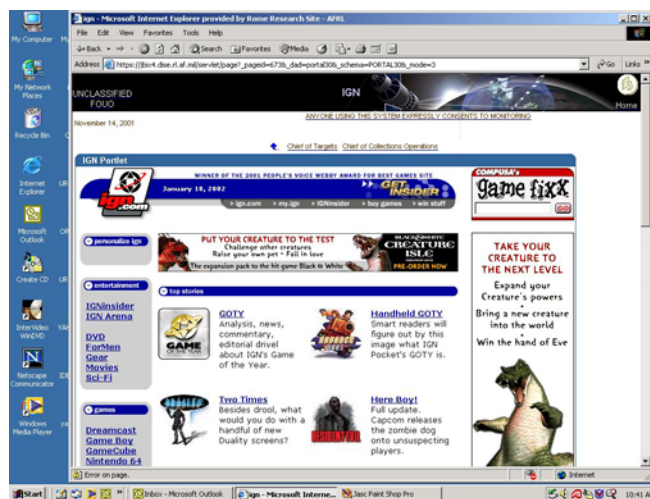


Figure 13 IGN.COM Being Pushed Through JBIX4

URL Services can be effectively used with the COMAFFOR page. For example, instead of forcing the user to click on the image to launch the application, the application will be launched upon selecting the tab. In addition, the URL services can take advantage of Oracle's single sign-on so that once the user authenticates with portal – no further authentication will be required. The single sign-on server maps the user's portal authentication to any application's authentication that is configured with the sign-on server. In order to implement these capabilities, work still needs to be done with both the single sign-on server and configuring URL Services to work with PKI certificates.

4.6.2 Customer Feedback Portlet

SOW 4.1.5 Work with the AC2ISRC, CAOCX, C2B, AFRL, ESC, Nellis, Military Battle Laboratories, and SWC, and other Government facilities to identify Information Exchange Requirements (IER) for the purpose of experimentation in the JBI-DT.

One of the portlets implemented from the PDK was Customer Feedback. The portlet can be accessed from the user *feedback link* on the JXP home page. This web-based form allows the user to provide any recommendations to the portal development team. All responses are stored in the database. The portlet as delivered in the PDK did not include the Customer Email field. The provider.xml file was modified to include the field and it was also added to the database. A user can also submit comments and recommendations via the Configuration Management DataBase (CMDB) link found on the Commander, Air Force Forces page.



Figure 14 Customer Feedback Page

4.7 Securing JXP

To properly secure JXP, a combination of Apache directives and Oracle features must be used. Portal 3.0.8.9.8 is built upon Apache 1.3.12. To prevent access to pages such as the Oracle root page, the appropriate directives in the httpd.conf were set. Oracle has extended Apache by providing a Mod_PLSQL Apache Plug-in. Apache serves as the listener for handling http/https requests. The Mod_PLSQL gateway does the data transfers between Apache and the database. This gateway has also been used to restrict access to the portals on jbix3 and jbix4. By specifying specific Internet protocol (IP) addresses or subdomains in the plsql.conf file, access can be restricted to individual hosts and subnets.

Several Oracle features have also been employed to restrict access to particular regions of the portal depending on who has authenticated. Two examples are provided. The first illustrates additional links being made available depending on user identity.



Figure 15 Public User's View of the Role Portlet

The next figure shows the roles that user jbiadmin can access.



Figure 16 JBIADMIN's View of the Role Portlet

Notice the addition of the *Update Role* link. This link takes jbiadmin to a page where he can customize the Portal Administrator page with a choice from several administrator applications. This illustrates another example of security provided by the portal. Depending on the user privileges, the user can view the page, add content only, add or remove content, change the page style, edit existing content, or have full control over the page. In this particular example, jbiadmin has the ability to add or remove content from the Portal Administrator page. He can only view the rest of the pages in the same manner that a public user can. The next figure shows the roles that the portal30 can access. Notice the addition of the *Homeland Defense* link. Also notice the addition of the *customize* link in the title bar. This user can also change the title of the portlet.

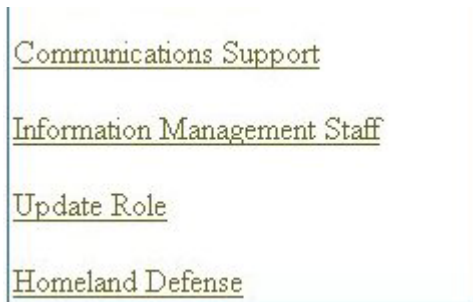


Figure 17 Portal30's View of the Role Portlet

Portal also provides security over individual tabs on a page. For example, the next figure shows some of the tabs a public user can see on the Commander, Air Force Forces page.

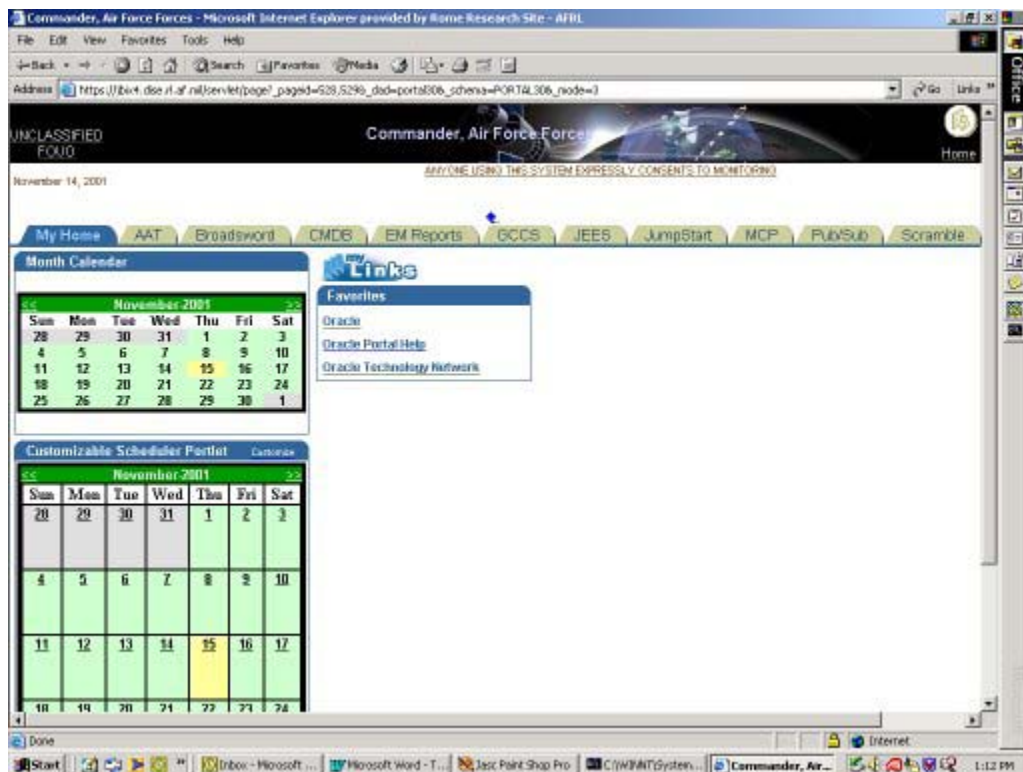


Figure 18 Public User's View of Page

The next figure shows the tabs that an authenticated user can view. Notice the addition of the CMAPI tab. CMAPI is a mapping application that the public user is prohibited from viewing.

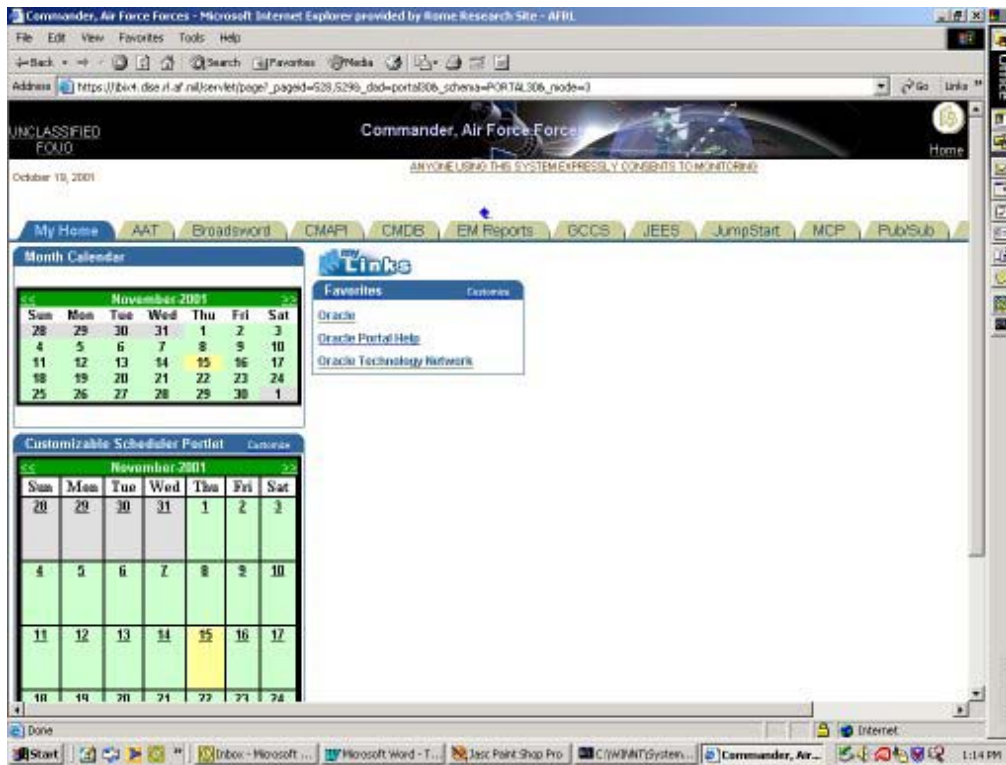


Figure 19 Authenticated User's View of Page

5. Configuration Management

SOW 4.1.4 Establish, record, and analyze performance measurements in the JBI-DT to baseline operational performance of C2ISR operational processes, hardware, and software components.

SOW 4.1.6 Perform IT system integration within the JBI-DT to provide new infrastructure and functional capabilities, and then return to previous configurations of JBI-DT. Participate in JBI-DT Configuration Management, IT system backup, and restoration to accomplish these JBI-DT incremental experiments and configuration rollbacks.

SOW 4.1.10 Conduct JBI-DT demonstrations and experiments as determined by the Government.

Numerous configuration management (CM) practices have been established in the C2TC. All of the equipment has been inventoried. Engineering logbooks have been placed by each of the machines to record all hardware and software changes. Startup and shutdown procedures have been developed for the portal systems and kept in a centralized notebook. Backup scripts have been developed for both the systems as well as the database. System backups are done weekly. Database-only backups are performed as required. Operating system and database security patches are applied as necessary.

Auditing and performance features have been examined. The portal has extensive auditing capabilities. Auditing can be performed by event or object. Common charts and canned queries to common auditing questions are provided. Oracle also provides a portlet-timing feature that displays the response time for the portlet to execute and return data.

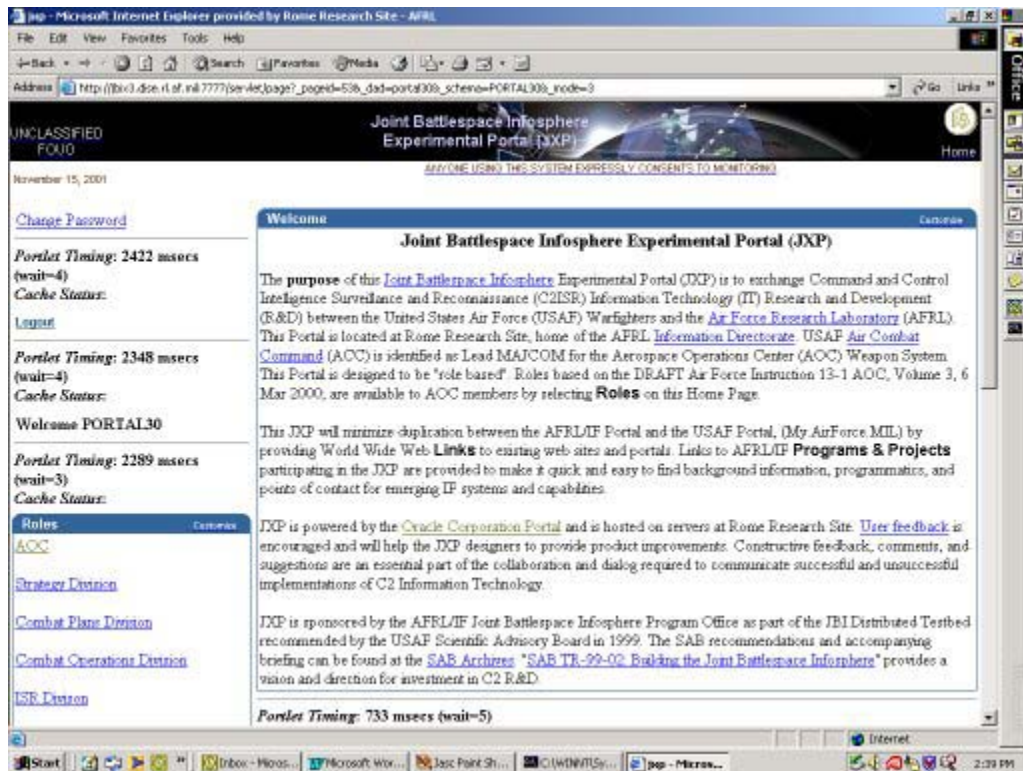


Figure 20 Portal Home Page with Timing Enabled

6. SIPRNET Migration

SOW 4.1.11 Perform technical requirement analysis to assure infrastructure conflicts are minimized during experimentation. This includes network traffic analysis, loading studies, and coordination with National-level network operation centers.

Plans are being developed to migrate the portal to SIPRNET. The architecture will be similar to jbx4. Initial content will consist of similar links and applications that are currently on jbx4. Not all unclassified sites will have a SIPRNET presence. Once the portal is established, content will be updated to include new information sources and applications not available over the Internet.

The plan is for the Air Force DoDIIS Infrastructure (AFDI) and the Defense Information Infrastructure Common Operating Environment (DII COE) to provide the security infrastructure. This is highly dependent on the versions of Solaris and Oracle that DII COE supports. The portal will be hosted on jbx3 and the machine will be completely rebuilt. The portal will be located in the C2TC.

7. Oracle 9i Beta Program

From March through July 2001, RRS/IFS along with Oracle's Advanced Products Group (APG) participated in the Oracle 9i Beta Program. The effort was conducted in the C2TC using jbox0. The objective of the test was to focus on "network database security. As a result of participating in the program, the Government was able to get an early look at the 9i software and directly interact with Oracle engineers on critical security issues. Refer to the press release in Appendix E for more information.

8. Conclusion

At the beginning of the project, Mr. Charles Flynn, TO-03 Program Manager, established goals for the JXP TO. Most were either partially or completely met. As was discovered, some were not feasible. The list of the JXP goals is provided here for reference. Each is discussed in the paragraphs that follow.

JXP Goals

- Build Role Based Portal for C2ISR Users
- Use Commercial Off The Shelf (COTS) Netscape or Explorer browser
- Work through USAF Firewalls on HTTP (HTTPS) Protocol
- Use USAF-Licensed COTS: Oracle 9iAS and Oracle 8i & 9i
- Impose no additional burden to System Administrators
- Require no new hardware or software in Operations Cells
- Integrate and Demonstrate Research and Development (R&D) Applications with SOR
- Users can logon to Portal from any network workstation
- Provide centralized Database Administration (DBA) and Portal Administration on Server

Goal: Build Role Based Portal for C2ISR Users

Goal: Integrate and Demonstrate Research and Development (R&D) Applications with SOR

The Oracle Portal is a sophisticated product built upon a very strong database. The Portal is not an easy product to use and the learning curve is rather steep. It took approximately two months to implement the use of PKI certificates. Requests for assistance have been received from the United Kingdom, Venezuela, Defense Financial and Accounting System (DFAS) and Oracle itself. The strengths of the product come from the security leveraging both from the database and Apache as well as from the flexible architecture built around portlets. The full benefits of the portlet centric architecture have yet to be realized. A strong knowledge of Oracle is necessary to take full advantage of the portal's features.

Under TO-03 a role-based portal was successfully implemented. The AOC role brought together several legacy and newly developed C2ISR applications. This task however has not been completed. More work must be done with URL services and Oracle's single sign-on server. This task will not be complete until the user can directly access each of the applications with only a single authentication. Additionally, the applications must be pushed to the user upon selecting the application's tab. Currently, the user must authenticate with each application individually and must then click on a link to access it.

Goal: Use Commercial Off The Shelf (COTS) Netscape or Explorer browser

The portal can be accessed from both Netscape and Internet Explorer browsers. The CMAPI application requires a properly configured Java plug-in. Instructions are provided on the portal.

Goal: Work through USAF Firewalls on HTTP (HTTPS) Protocol

The portal has yet to be tested through firewalls because the HTTPS protocol has only recently been configured. Some problems may be encountered because the RRS firewalls may not be configured to allow traffic by the necessary ports and protocols. This can be alleviated by either creating “firewall holes” or moving the portal within the RRS network topology so that “firewall holes” do not need to be created or the number can be minimized.

Use USAF-Licensed COTS: Oracle 9iAS and Oracle 8i & 9i

At the present time, these are the only COTS products being used other than Windows 2000 Advanced Server and Solaris. If the portal is migrated to the Oracle 9i database, then additional licenses will be needed to implement new features such as label security.

Goal: Impose no additional burden to System Administrators

Goal: Provide centralized Database Administration (DBA) and Portal Administration on Server

A portal cannot be implemented without putting additional burdens on a system administrator. Currently jbix3 and jbix4 are additional systems to maintain. Backup scripts for both the system and the database need to be developed. Patches for Oracle and IAS/Portal need to be kept current. New releases of Oracle and Portal will need to be installed. These functions are not trivial; nor is exporting the portal from one machine to another. Difficulties were encountered when building jbix4 using the import/export scripts.

Currently all administration is centralized. However, if the full potential of the portal is realized, central administration is not necessary or desired. Through the use of portlets, applications can be developed and maintained at remote locations. Portal administrators would *provide* the portlets to other administrators who can then include them into their portals. Using this approach, when a portlet is upgraded, an administrator would only need to *refresh* the portal provider to access the latest versions.

Goal: Require no new hardware or software in Operations Cells

No additional hardware or software will be required to access the portal. Both jbix3 and jbix4 are good platforms for the development and fielding of the portal.

Goal: Users can logon to Portal from any network workstation

This goal was achieved when Portal was upgraded from version 3.0.6.6.5 to 3.0.8.9.8 and the self-registration portlet was implemented.

Appendix A – Oracle Technical Assistance Request Number 1939945.999

TAR Number 1939945.999 Open Date 15-OCT-01 17:53:11
Support Identifier 2193548 Name Robert Gann
Priority 2 Last Update 15-NOV-01 07:36:08
Product Portal Product Version 3.0.8.9.8
Platform MS Windows 2000 Detailed Status Hard Close
TAR Reference n/a BUG Reference 1714880

Abstract

Cannot cancel when editing an application

Resolution History

15-OCT-01 17:53:11 GMT

Can you easily recover from, bypass or work around the problem? = NO
Does your system or application continue normally after the problem occurs? = NO
Are the standard features of the system or application still available; is the loss of service minor? = NO

Describe the problem you are having in detail. Include any notes, guides:
When I try to edit an application and select cancel I get the errors below. I have a DAD called JBIX4 defined. The URL in the error message is messed up. If you start with the https and continue, the URL works fine. In a related manner, when I select click on pages on my site, occasionally, but too frequently, it comes back and it says it can't find the page. On our Solaris portal, this doesn't happen. One other piece of information. I have the following statement in my httpd.conf file.
Redirect /jxphome https://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome
Thanks.

MON, 15 OCT 2001 17:37:25 GMT

No DAD configuration Found
DAD name:
PROCEDURE : /jbix4.dise.rl.af.mil/servlet/page
URL :
http://jbix4.dise.rl.af.mil:443/pls/portal30/https://jbix4.dise.rl.af.mil/servlet/page?_pageid=3,22&_dad=portal30&_schema=PORTAL30&_mode=3&p_render=LIST&p_otype=APP&p_octx=JBI.APP_JXP&p_action=&p_caller=PORTLET&p_domain=wwc&p_sub_domain=app

exp&p_rpth=49_APPLICATIONEXPLORER_790592&p_orderby=&p_request=
&p_min_row=1&p_max
_rows=49&p_page_number=1

PARAMETERS :

=====

ENVIRONMENT:

=====

PLSQL_GATEWAY=WebDb

GATEWAY_IVERSION=2

SERVER_SOFTWARE=Oracle HTTP Server Powered by Apache/1.3.12
(Win32)

ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.24

GATEWAY_INTERFACE=CGI/1.1

SERVER_PORT=443

SERVER_NAME=jbix4.dise.rl.af.mil

REQUEST_METHOD=GET

QUERY_STRING=_pageid=3,22&_dad=portal30&_schema=PORTAL30&_mo
de=3&p_render=LIST&p

_otype=APP&p_octx=JBI.APP_JXP&p_action=&p_caller=PORTLET&p_domai
n=wwc&p_sub_doma

in=appexp&p_rpth=49_APPLICATIONEXPLORER_790592&p_orderby=&p_re
quest=&p_min_row=1

&p_max_rows=49&p_page_number=1

PATH_INFO=/portal30/https://jbix4.dise.rl.af.mil/servlet/page

SCRIPT_NAME=/pls

REMOTE_HOST=

REMOTE_ADDR=192.5.148.83

SERVER_PROTOCOL=HTTP/1.1

REQUEST_PROTOCOL=HTTPS

REMOTE_USER=

HTTP_CONTENT_LENGTH=

HTTP_CONTENT_TYPE=

HTTP_USER_AGENT=Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)

HTTP_HOST=jbix4.dise.rl.af.mil

HTTP_ACCEPT=image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword,

Text continued in next action...

15-OCT-01 17:54:04 GMT

Text continued from previous action...

/

HTTP_ACCEPT_ENCODING=gzip, deflate

HTTP_ACCEPT_LANGUAGE=en-us
HTTP_ACCEPT_CHARSET=

HTTP_COOKIE=portal30=3.0,en,us,AMERICA,950731D8A7F1EC0B30FFD8D
3F0C61BB49E20519A6
7785E88000698682C92814518EADD3629F69D684BC17B89F3528FBD406AF
5FDA051CA6A6742B6F8D
BE40BA9D0E0FD70F27C4DADB4632B77C5EAA7130A8ED2CDD98600DC6
D2A0E559CADA0B0;
portal30_sso=3.0,en,us,AMERICA,E9AD83E8B449E3710CCB6B965D1A29C1
99CA4E8491A35AB63
4EBB53FC816703F56DB97F8471A457E5562A6671EE8F3265C0CDDDF961D
43384BEF5CBBF450A7CE8
69C2BC91348EC02CB92FEF52CC98390091647CB719995E3
Authorization=
HTTP_IF_MODIFIED_SINCE=

HTTP_REFERER=https://jbix4.dise.rl.af.mil/pls/portal30/PORTAL30.www_builder.show
?p_module_id=1953487619&p_version=9&p_section=1&p_save_version=10&p_mode=EDIT&p_app_name=APP_JXP&p_redirect_url=https%3A%2F%2Fjbix4.dise.rl.af.mil%2F servlet%2Fp age%3F_pageid%3D3%2C22%26_dad%3Dportal30%26_schema%3DPORTAL3 0%26_mode%3D3%26p_re nder%3DLIST%26p_otype%3DAPP%26p_octx%3DJBI.APP_JXP%26p_action %3D%26p_caller%3DPO RTLET%26p_domain%3Dwwc%26p_sub_domain%3Dappexp%26p_rpth%3D4 9_APPLICATIONEXPLORER _790592%26p_orderby%3D%26p_request%3D%26p_min_row%3D1%26p_max _rows%3D49%26p_page _number%3D1

Provide any error numbers, or error text that you are receiving. Include a none

Is this a new install, or migration? ###
Migration

If migrating, what are the full versions of WebDB/Portal, and the database I did exported from version 3.0.8.9.8 on Solaris.

Is the database local, or remote? ###
Local - same ORACLE_HOME

Is WebDB installed in an existing Oracle_Home? If so, on which product's O

no

What other Oracle products exist on the server?

Oracle 8.1.7

How many database instances are on this server?

One

List the values for the following environment settings: ORACLE_HOME,

WV_GAT

ORACLE HOME - D:\ORACLEIAS\iSuites

WV_GATEWAY_CFG -

D:\ORACLEIAS\iSuites\Apache\modplsql\cfg\wdbsvr.app

There is no TNS_ADMIN or CLASSPATH

PATH is very long

Can you connect to the database through SQL*Plus in the WebDB/Portal home?

Yes

Contact me via : Electronic support services

15-OCT-01 18:06:02 GMT

New info : Here is some info from the mod_jserv.log file.

[15/10/2001 17:34:38:734] (EMERGENCY) ajp12: connection fail

[15/10/2001 17:34:38:734] (ERROR) an error returned handling request via protocol "ajpv12"

[15/10/2001 17:34:40:812] (EMERGENCY) ajp12: can not connect to host 127.0.0.1:8007

15-OCT-01 18:33:51 GMT

Is your Portal running OK otherwise (not editing or canceling from editing an application)?

The error seems to indicate a problem with your JServ not Portal.

Is this happening at all times or just while editing an application imported from the Solaris box?

Is it happening to just this application?

@cus

15-OCT-01 18:34:04 GMT

Email Update button has been pressed -- Sending email.

15-OCT-01 20:00:09 GMT

New info : The problem happens all of the time. The reason why I provided the editing, then cancel as an example is that it happens nearly all of the time. What is more disconcerting is that there are numerous times when I try to access a page, it does not appear and I get error messages very similar to what I shared with you. That is actually the problem I want to fix. Is the URL in the error part correct? If I highlight the part beginning with https, it works just fine.
Thanks.

17-OCT-01 13:33:19 GMT

Robert, we need to simplify this.
What exactly is the error and when does it occur. I need to be able to reproduce this in some way.

Should I look at the error while editing and cancelling out of an application or in general, while using Portal?

Which one is the error? The issue with the ajp12 protocol may not necessarily be related to the problem with the redirection issue or the incorrect URL.

I would recommend we address the java server error and the ajp12 protocol with a specific error that I can address.

While the JServ is supported by a different group, please take a look at the following notes in MetaLink and see if you can correct the AJP12 error:

Note:110540.1

Note:131327.1

Note:130748.1

@cus

17-OCT-01 13:33:30 GMT

Email Update button has been pressed -- Sending email.

17-OCT-01 14:45:04 GMT

New info : OK, when I click on an application to edit and then I click cancel, everytime it fails. I get a big error dump as follows. Please look at the URL entry. It appears wrong. It associates http with 443. If I copy the url

beginning with https it works just fine. I don't know what is going on at the beginning of the URL. It appears that some appending is going on or some table entry is corrupt - I don't know. There is a DAD defined for jbix4. I don't know why there is no DAD. OK now for the error. Thanks.

WED, 17 OCT 2001 14:43:21 GMT

No DAD configuration Found

DAD name:

PROCEDURE : /jbix4.dise.rl.af.mil/servlet/page

URL :

http://jbix4.dise.rl.af.mil:443/pls/portal30/https://jbix4.dise.rl.af.mil/servlet/page?_pageid=3,22&_dad=portal30&_schema=PORTAL30&_mode=3&p_render=LIST&p_otype=APP&p_octx=JBI.APP_JXP&p_action=&p_caller=PORTLET&p_domain=wwc&p_sub_domain=appexp&p_rpth=49_APPLICATIONEXPLORER_790592&p_orderby=&p_request=&p_min_row=1&p_max_rows=49&p_page_number=1

PARAMETERS :

=====

ENVIRONMENT:

=====

PLSQL_GATEWAY=WebDb

GATEWAY_IVERSION=2

SERVER_SOFTWARE=Oracle HTTP Server Powered by Apache/1.3.12 (Win32)

ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.24

GATEWAY_INTERFACE=CGI/1.1

SERVER_PORT=443

SERVER_NAME=jbix4.dise.rl.af.mil

REQUEST_METHOD=GET

QUERY_STRING=_pageid=3,22&_dad=portal30&_schema=PORTAL30&_mode=3&p_render=LIST&p_otype=APP&p_octx=JBI.APP_JXP&p_action=&p_caller=PORTLET&p_domain=wwc&p_sub_domain=appexp&p_rpth=49_APPLICATIONEXPLORER_790592&p_orderby=&p_request=&p_min_row=1&p_max_rows=49&p_page_number=1
PATH_INFO=/portal30/https://jbix4.dise.rl.af.mil/servlet/page
SCRIPT_NAME=/pls
REMOTE_HOST=
REMOTE_ADDR=192.5.148.85
SERVER_PROTOCOL=HTTP/1.1

REQUEST_PROTOCOL=HTTPS
REMOTE_USER=
HTTP_CONTENT_LENGTH=
HTTP_CONTENT_TYPE=
HTTP_USER_AGENT=Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
HTTP_HOST=jbix4.dise.rl.af.mil
HTTP_ACCEPT=image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
HTTP_ACCEPT_ENCODING=gzip, deflate
HTTP_ACCEPT_LANGUAGE=en-us
HTTP_ACCEPT_CHARSET=
HTTP_COOKIE=SITESERVER=ID=224cb1c9e0c6d22751dc775a9e1de494;
portal30=3.0,en,us,AMERICA,04193673475D325F02680DF45661E5EC5D47D0
F6895E9B24DAF6C
FC264357CE207281BC60689C368CE426D89BD511071F0513E3E7ECAFD4
422E7E056D5CE647A26B9
4A0CBB8D5897371753BF18DC9FEA92157316D66C75878F8D0EC7F07B17E
;
portal30_sso=3.0,en,us,AMERICA,5ADEFDCC8666CA7B617A901CF3DE8EE
9D5A0B542E9229766D
Text continued in next action...

17-OCT-01 14:46:08 GMT

Text continued from previous action...

4858404326F7DC6797F4F1BEF934A1933F49459A2D8C633CF68ABB997320
AEE346BFF5FC485FB6D9
3A657F72508387CC5F3DE5AD49498C298C875D6A36542A3
Authorization=
HTTP_IF_MODIFIED_SINCE=

HTTP_REFERER=https://jbix4.dise.rl.af.mil/pls/portal30/PORTAL30.www_builder.show
?p_module_id=1953487619&p_version=9&p_section=1&p_save_version=10&p_mode=EDIT&p_app_name=APP_JXP&p_redirect_url=https%3A%2F%2Fjbix4.dise.rl.af.mil%2F servlet%2Fpage%3F_pageid%3D3%2C22%26_dad%3Dportal30%26_schema%3DPORTAL30%26_mode%3D3%26p_render%3DLIST%26p_otype%3DAPP%26p_octx%3DJBI.APP_JXP%26p_action%3D%26p_caller%3DPORTLET%26p_domain%3Dwwc%26p_sub_domain%3Dappexp%26p_rpth%3D49_APPLICATIONEXPLORER_790592%26p_orderby%3D%26p_request%3D%26p_min_row%3D1%26p_max_rows%3D49%26p_page

_number%3D1

17-OCT-01 15:52:36 GMT

Can you tell me the full URL you are trying to redirect and what is that url pointing to? What is url/page/jxphome? Specifically, what is jxphome?

I see that the line in the httpd.conf files is:

Redirect /jxphome https://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome

What happens if you enter this url from the browser:

https://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome

I'll have to try redirecting something similar on my machine and try to click cancel to test the results, but I need to know what I'm going to redirect first. Is this a public page?

I guess I need to know the relationship between the redirection you have established:

Redirect /jxphome https://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome and the application you are editing but fails when you click cancel.

I tried redirecting to a simple public page and that works.

@cus

17-OCT-01 15:53:22 GMT

Email Update button has been pressed -- Sending email.

17-OCT-01 16:35:04 GMT

New info : jxphome is our homepage. If I type out the full URL, I go to the homepage. The reason why we are using the redirect is so the user does not have to type the entire URL. https://jbix4.dise.rl.af.mil/jxphome is much easier than https://jbix4.dise.rl.af.mil/pls/portal30/url/page/homepage.

Unfortunately you cannot get to the homepage because it is behind a firewall.

The redirect from the httpd.conf file is

Redirect /jxphome https://jbix4.dise.rl.af.mil/pls/portal30/url/page/jxphome

The redirect appears to be working fine, at least on the surface. Typing it will take you to the homepage.

Most of the applications that I build are dynamic pages using the Create New list from the navigator.

Are you thinking that the redirect has something to do with it? Is the redirection not being handled correctly?

17-OCT-01 19:08:26 GMT

Robert, to be honest with you, I'm not sure the redirection has anything to do with it. You also have SSL enabled but I have not thought about this been a problem yet.

The redirection line in your httpd.conf is fine. In fact I tried the same thing here to access a page I created and it works.

See if you can isolate without so many
Try commenting out the redirect line from the httpd.conf file and see if that resolves anything.
Since you have this working on Solaris, you might want to compare config files.

Also check the database for invalid objects.

@cus

17-OCT-01 19:08:39 GMT

Email Update button has been pressed -- Sending email.

17-OCT-01 19:20:06 GMT

New info : May I ask a question? I don't think it has anything to do with redirection. How is that URL at the top of the error page formed? Could it have something to do with running ssodatan? If you could tell me how the URL is formed, we could then look at the table(s) and possibly see what's up.

22-OCT-01 14:11:33 GMT

I'm trying to find more on how the URL is formed but have not had luck on this. The URL is redirected internally and I'm not sure where it is stored or if it should be modified or if we support this.

You can verify the URLs entered during execution of the ssodatan command by viewing the content of the WWSEC_ENABLER_CONFIG_INFO\$ table.

We should first try to determine if SSL is causing this and perhaps remove the Redirect directive from the httpd.conf file.

Were you ever able to edit and then cancel from an application?
Did this start happening after implementing SSL?
Does this happen on any application or just one?
Is this application running successfully?

@cus

22-OCT-01 14:11:45 GMT

Email Update button has been pressed -- Sending email.

26-OCT-01 13:42:07 GMT

Any word on this?

What is the content of the WWSEC_ENABLER_CONFIG_INFO\$ table?
Have you tried running the ssodatan script with the correct parameters?

Have you made any changes to the httpd.conf file?

I posted a reply and some questions on Oct 22 but have not received a reply.

@cus

26-OCT-01 13:42:16 GMT

Email Update button has been pressed -- Sending email.

26-OCT-01 15:26:02 GMT

The customer has uploaded the following file via MetaLink:
httpd.conf

26-OCT-01 15:30:08 GMT

New info : I did not see the past update. Below I have answered the posted questions. I also provided you with my httpd.conf file as well. Any insight would be greatly appreciated. Thanks.

Robert Gann

Here are the answers to the questions.

Were you ever able to edit and then cancel from an application? I think so.

Did this start happening after implementing SSL? It has definitely always happened since SSL is up.

Does this happen on any application or just one? This occurs almost 100% of the time with all applications.

Is this application running successfully? Yes.

Have you tried running the ssodatan script with the correct parameters? Yes.

I have ran ssodatan several times.

Have you made any changes to the httpd.conf file?

Below I have provided the contents of the
WWSEC_ENABLER_CONFIG_INFO\$ table.
Contents of WWSEC_ENABLER_CONFIG_INFO\$
LSNR_TOKEN

jbix4.dise.rl.af.mil
SITE_TOKEN

42N8937H1346
SITE_ID

1346
LS_LOGIN_URL

https://jbix4.dise.rl.af.mil/pls/portal30_sso/portal30_sso.wwsso_app_admin.ls_login
URLCOOKIE_VERSION

v1.1
ENCRYPTION_KEY

13d7ee189a931447
ENCRYPTION_MASK_PRE

4BD7749E3EFC7863DFBAD23FED06F5BD
ENCRYPTION_MASK_POST

6DE6A02B132C1D11AE933E867A17333B
U
-
Y

26-OCT-01 15:34:16 GMT

Reviewing...

@wip

30-OCT-01 14:28:22 GMT

Robert, it looks like wwv_redirect.url() function (file wwv/wwvredir.plb) does not handle https correctly, or rather, does not handle https at all, it just happened that forms are using redirect on a regular basis comparing with other components, so any code using https and wwv_redirect.url() will fail.

This was reported in Bug# 1714880 logged against Portal 3.0.8.9.8

There is a patch available for Portal 3.0.8 in MetaLink that replaces the `www_redir.plb`

From MetaLink, click Patches and enter Patch Number: 1714880, Platform: MS Windows NT/2000 Server

The other option is to upgrade to Portal 3.0.9 where the fix is included.

As with any patches, please backup your data first.

Let me know if this helps.

@cus

30-OCT-01 14:29:13 GMT

Email Update button has been pressed -- Sending email.

30-OCT-01 18:31:03 GMT

New info : The patch may have done it. I tried to edit 60 applications then hit cancel every time, no failures. I do have a related question before you close the TAR. I tried the same application edit/cancel using the navigator but from a remote workstation and it failed. Is there a similar patch.

30-OCT-01 19:41:41 GMT

That patch is generic and could be applied to any platform on which Portal is installed.

However, I'm not sure you are referring to a different instance of Portal or just another machine from which you are logged in to Portal to edit/cancel an application.

This could be totally different since you now are dealing with another machine, IP address, and the server might be placing the restriction.

Is the error the same?

@cus

30-OCT-01 19:41:50 GMT

Email Update button has been pressed -- Sending email.

31-OCT-01 13:55:02 GMT

New info : Thank you for your help. I will work that issue later. For now I consider the issue closed.

31-OCT-01 13:56:02 GMT

Closed by customer

31-OCT-01 13:57:04 GMT

Closed by customer

15-NOV-01 07:36:08 GMT

TAR passed SCL review date. Setting to HCL.

Appendix B. JBIX4 Screen Shots

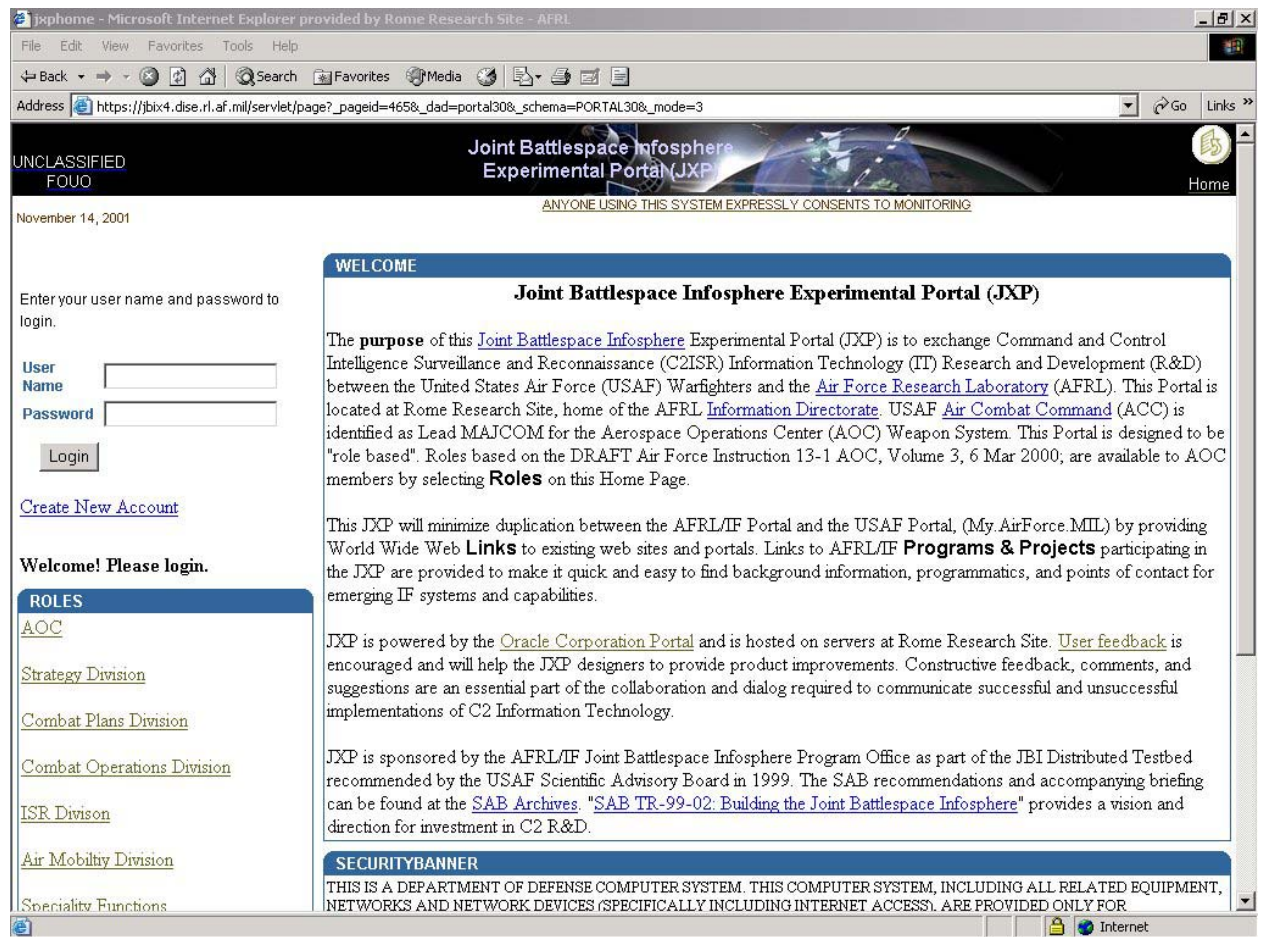


Figure B-1 JBIX4 Home Page

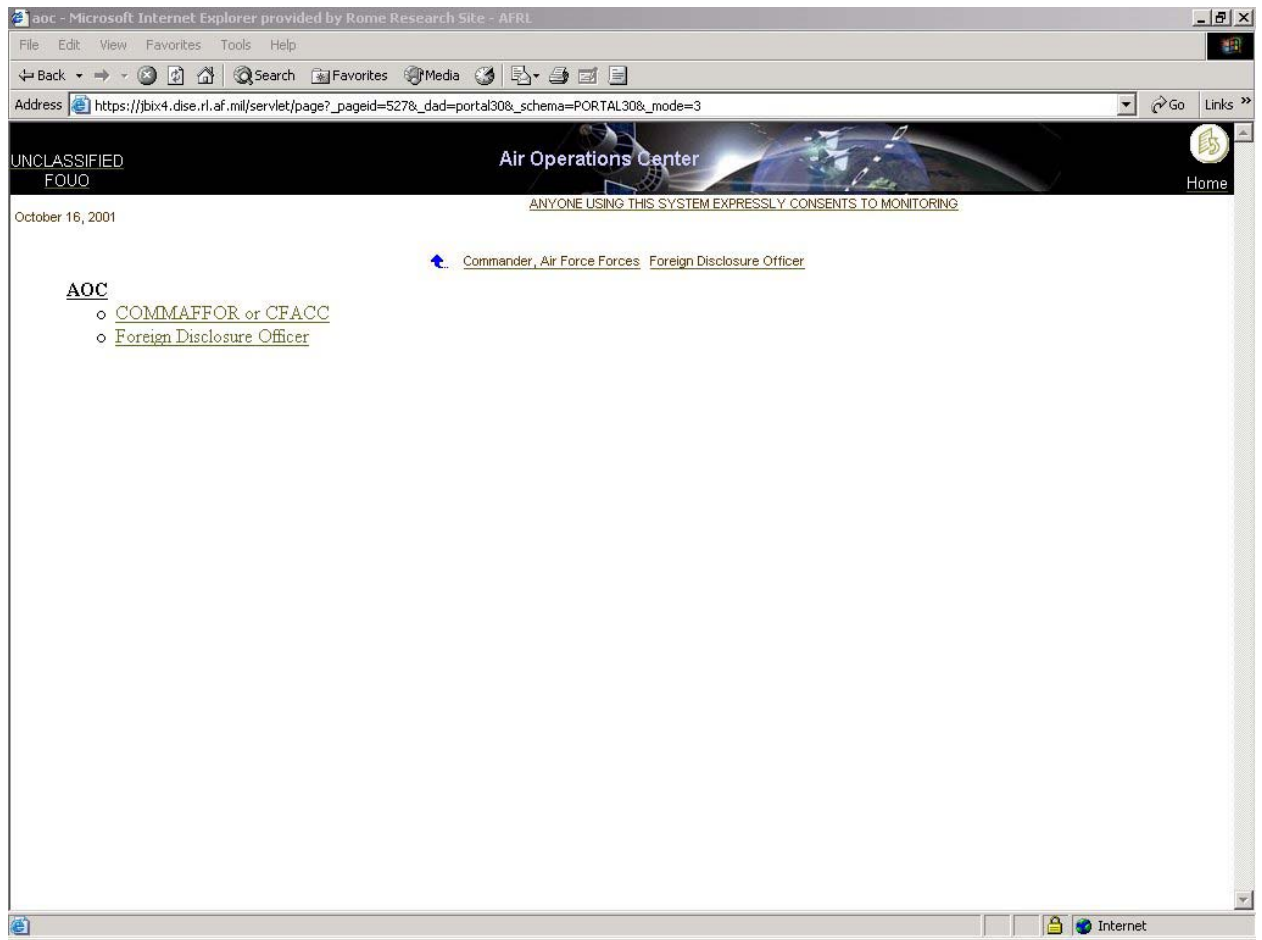


Figure B-2 Air Operations Center

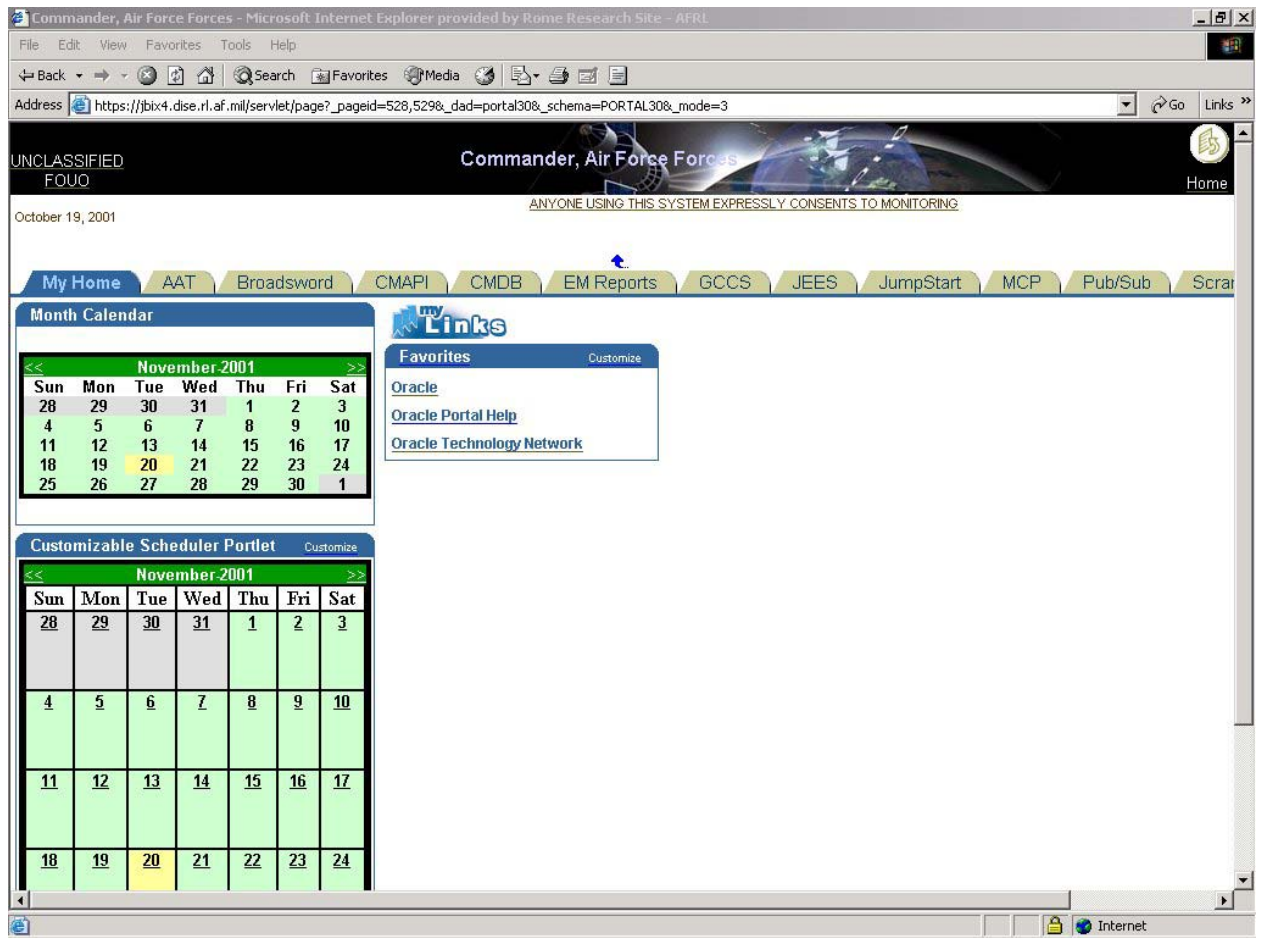


Figure B-3 Commander, Air Force Forces

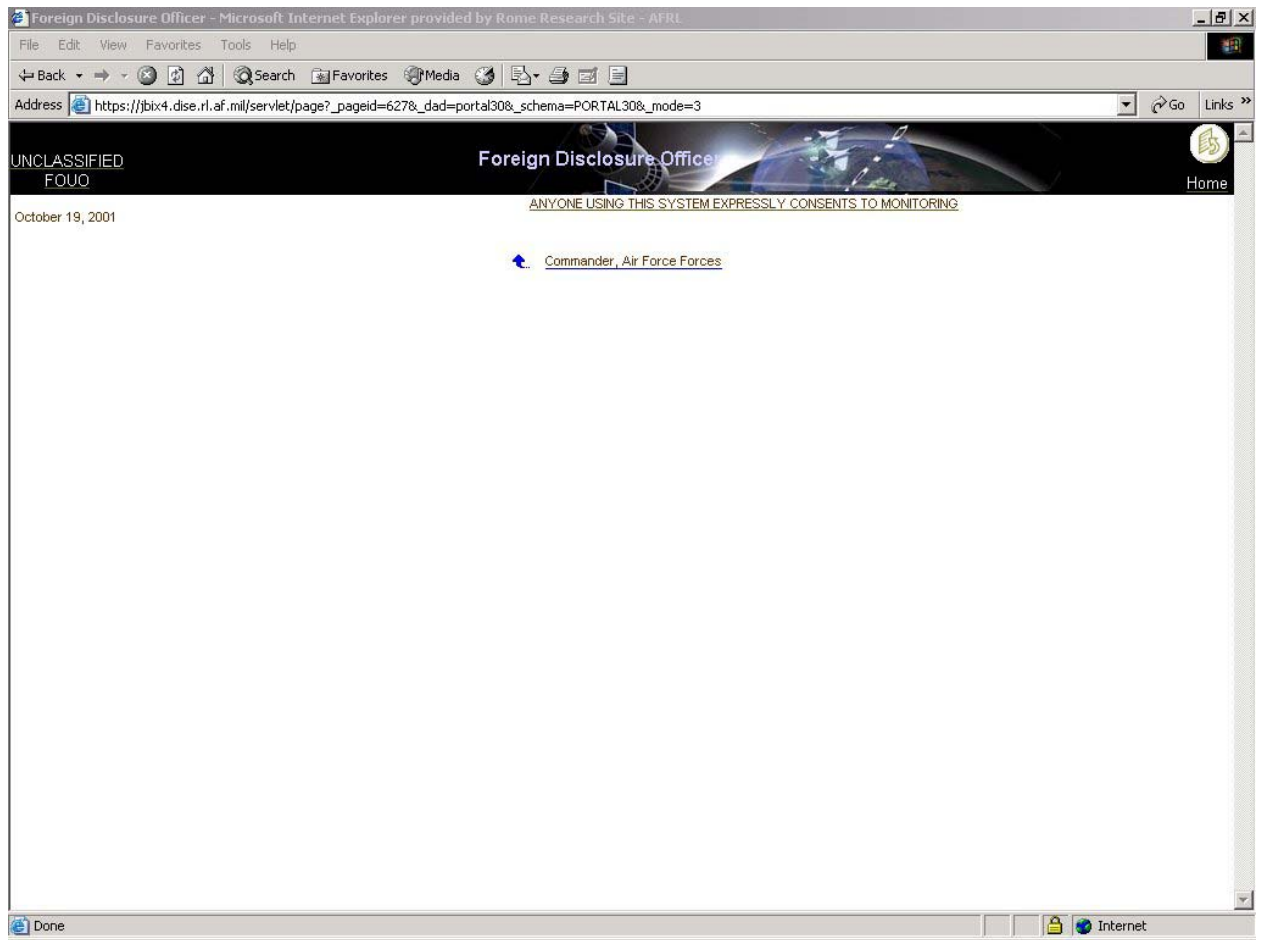


Figure B-4 Foreign Disclosure Officer

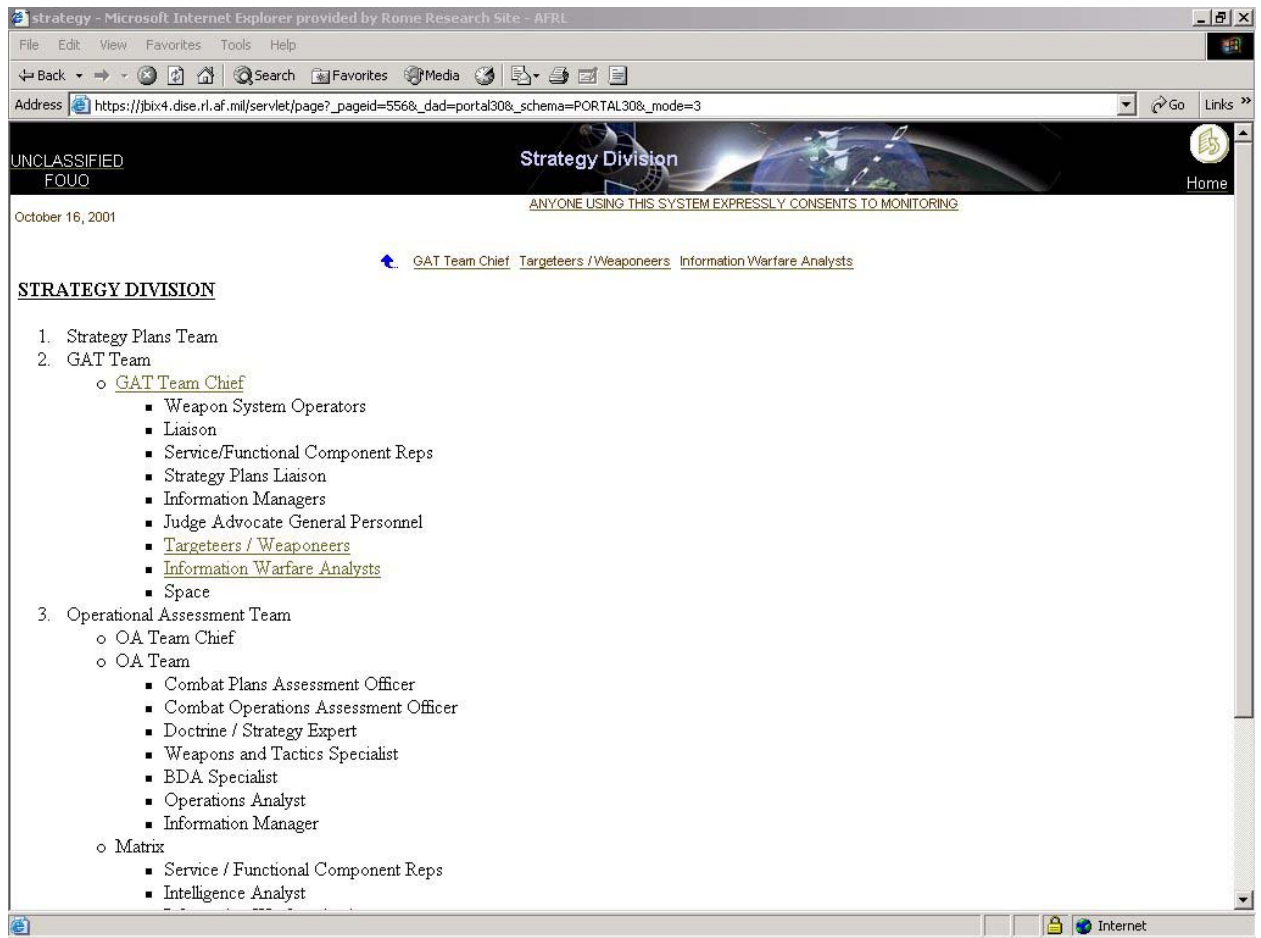


Figure B-5 Strategy Division

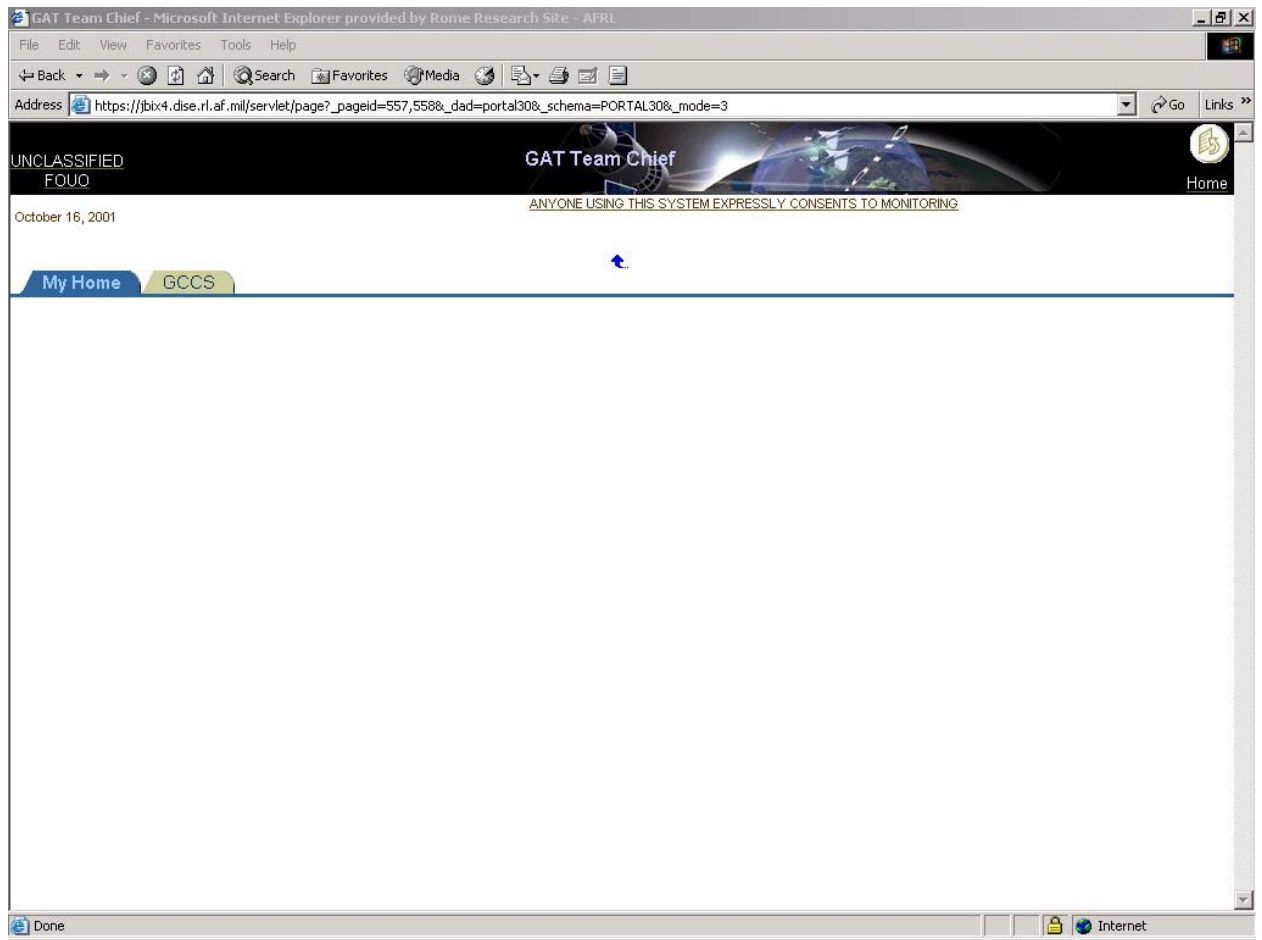


Figure B-6 GAT Team Chief

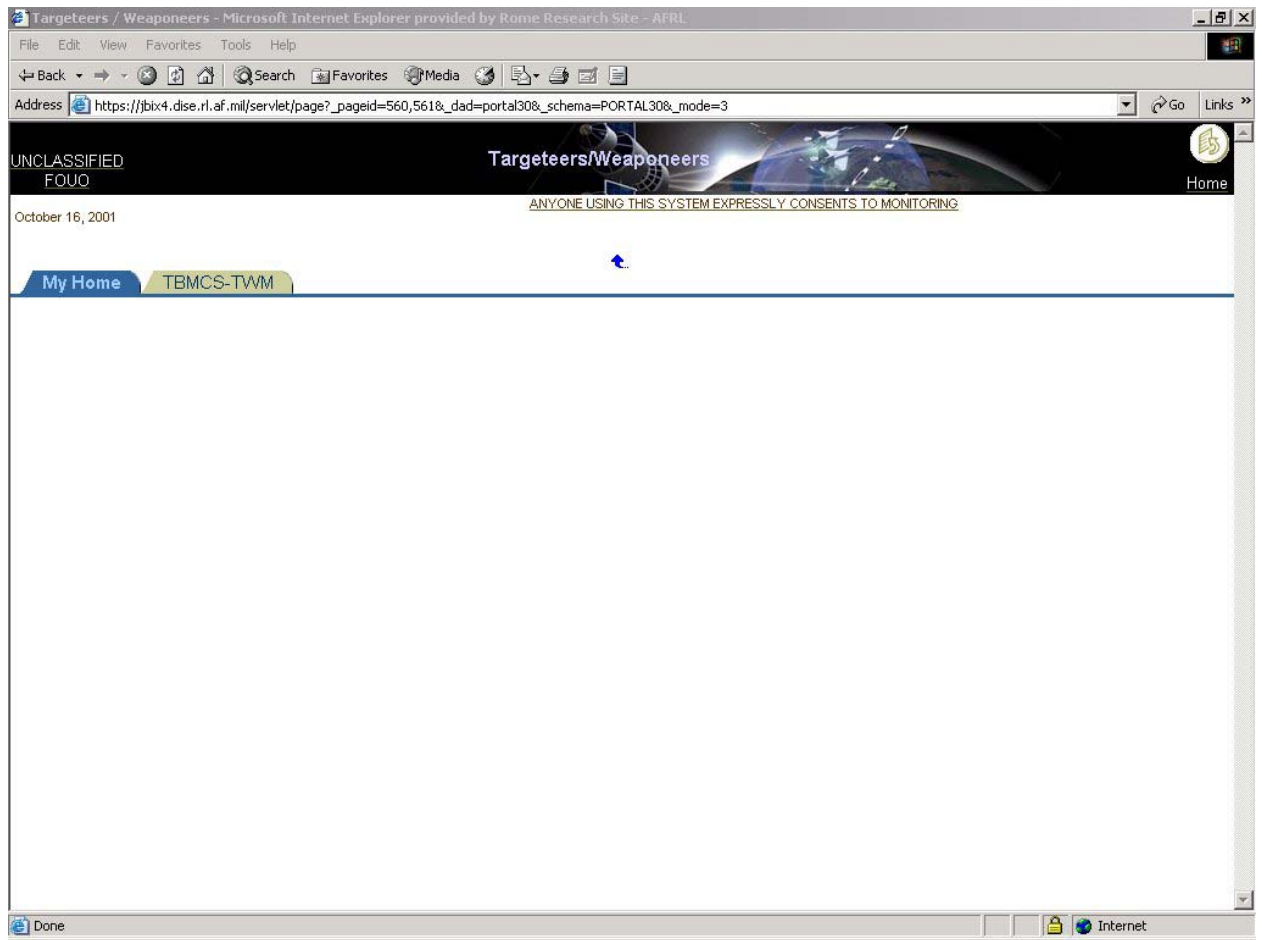


Figure B-7 Targeteers/Weaponers

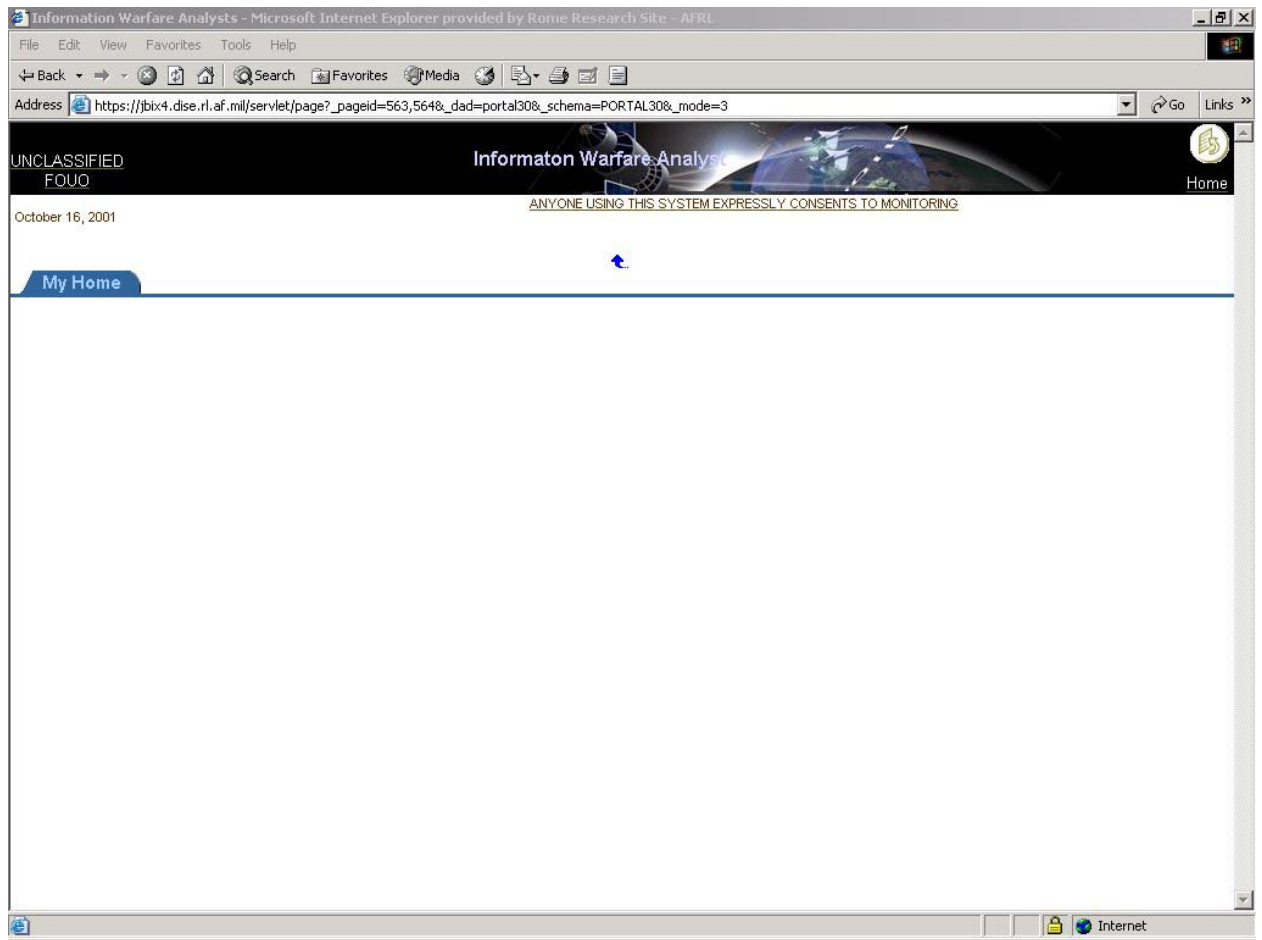


Figure B-8 Information Warfare Analysts

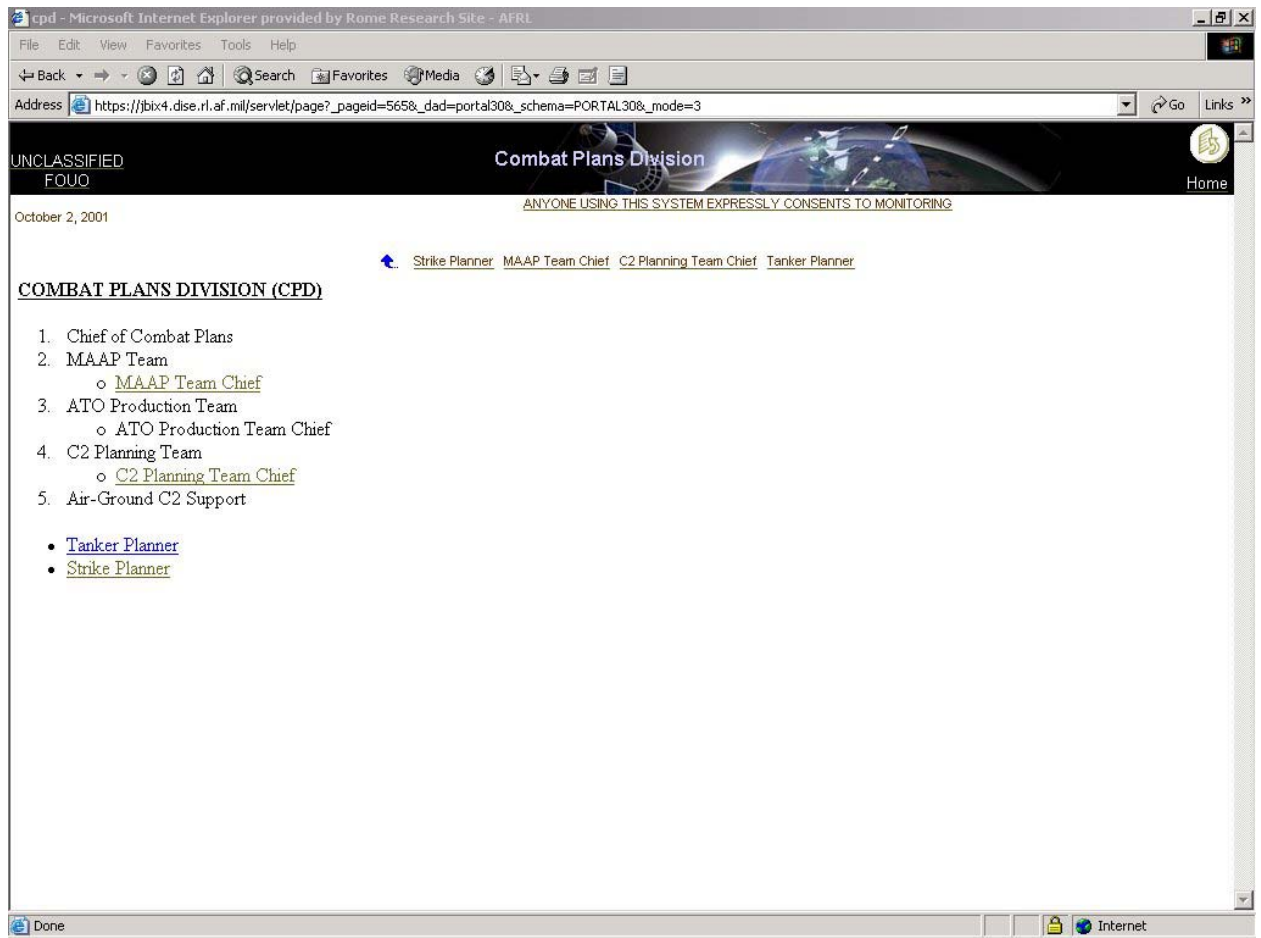


Figure B-9 Combat Plans Division

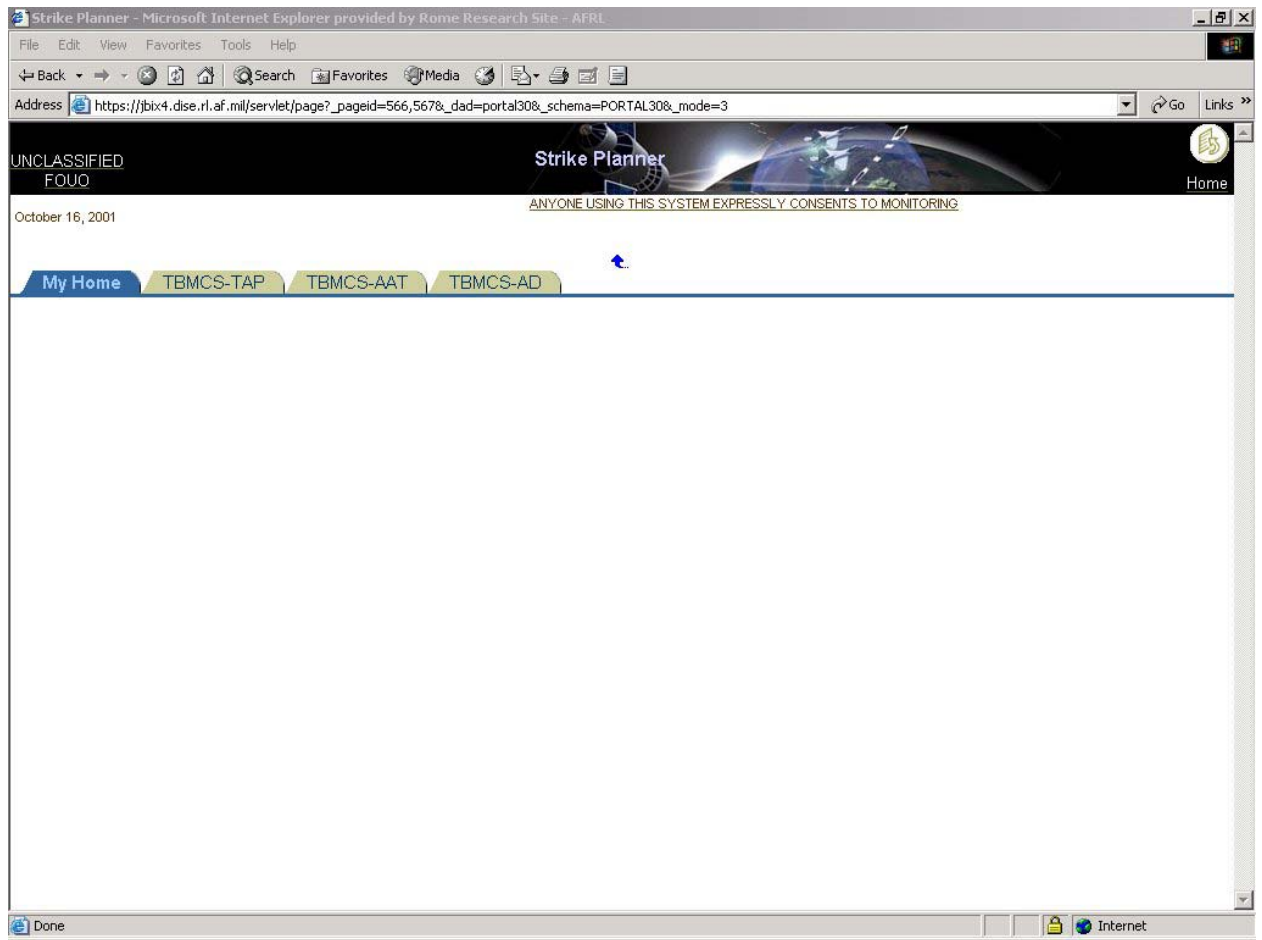


Figure B-10 Strike Planner

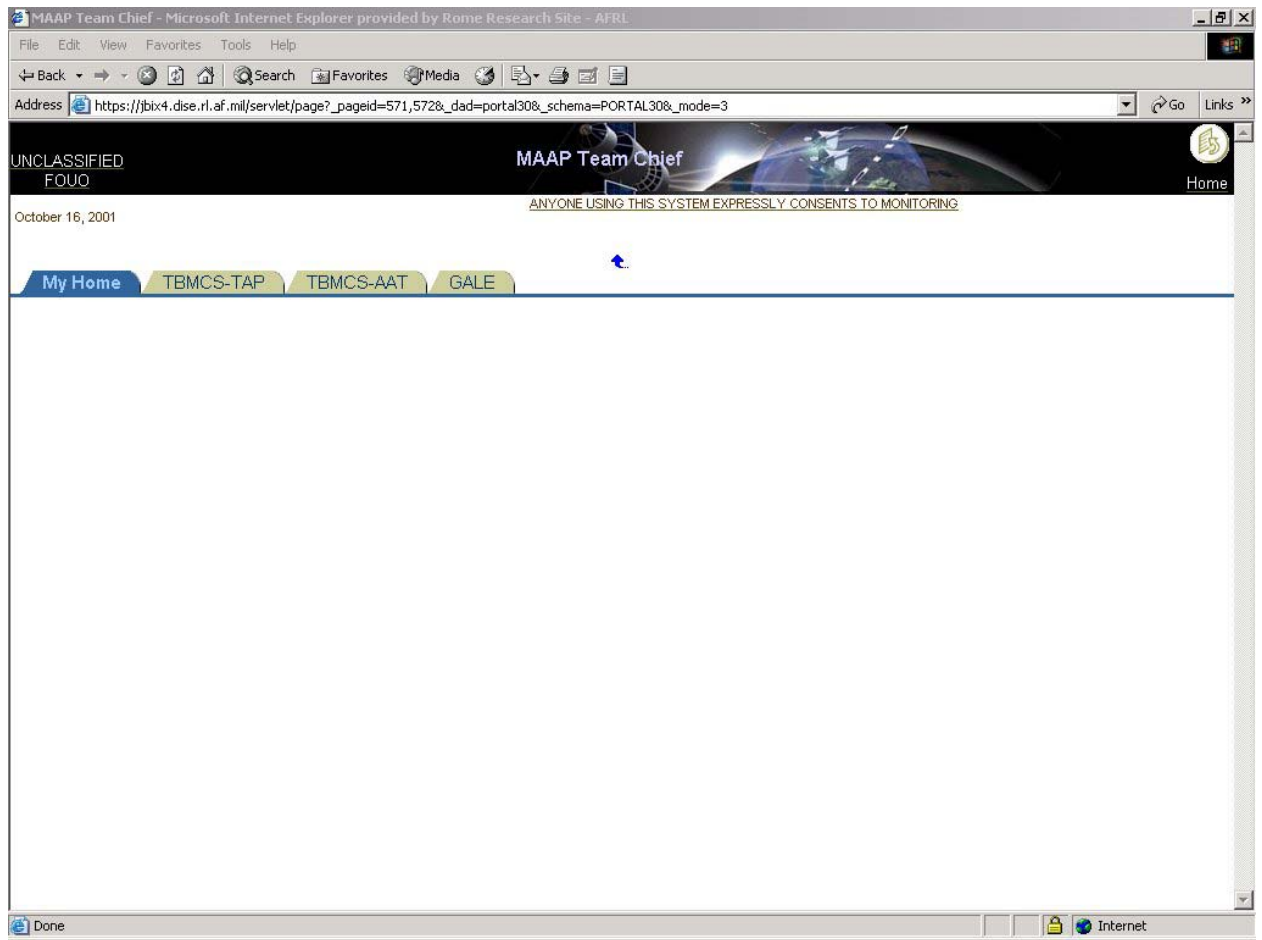


Figure B-11 MAAP Team Chief

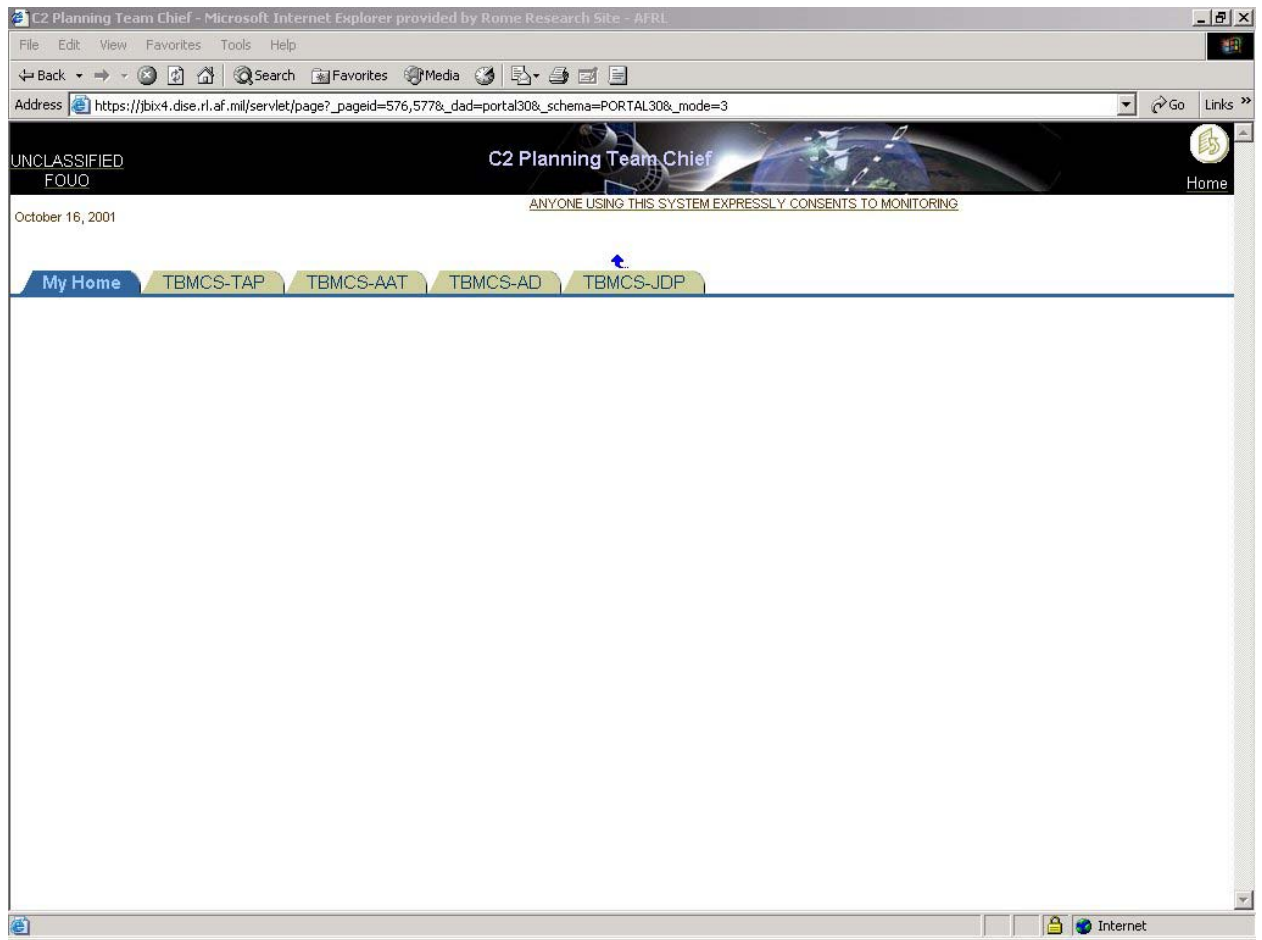


Figure B-12 C2 Planning Team Chief

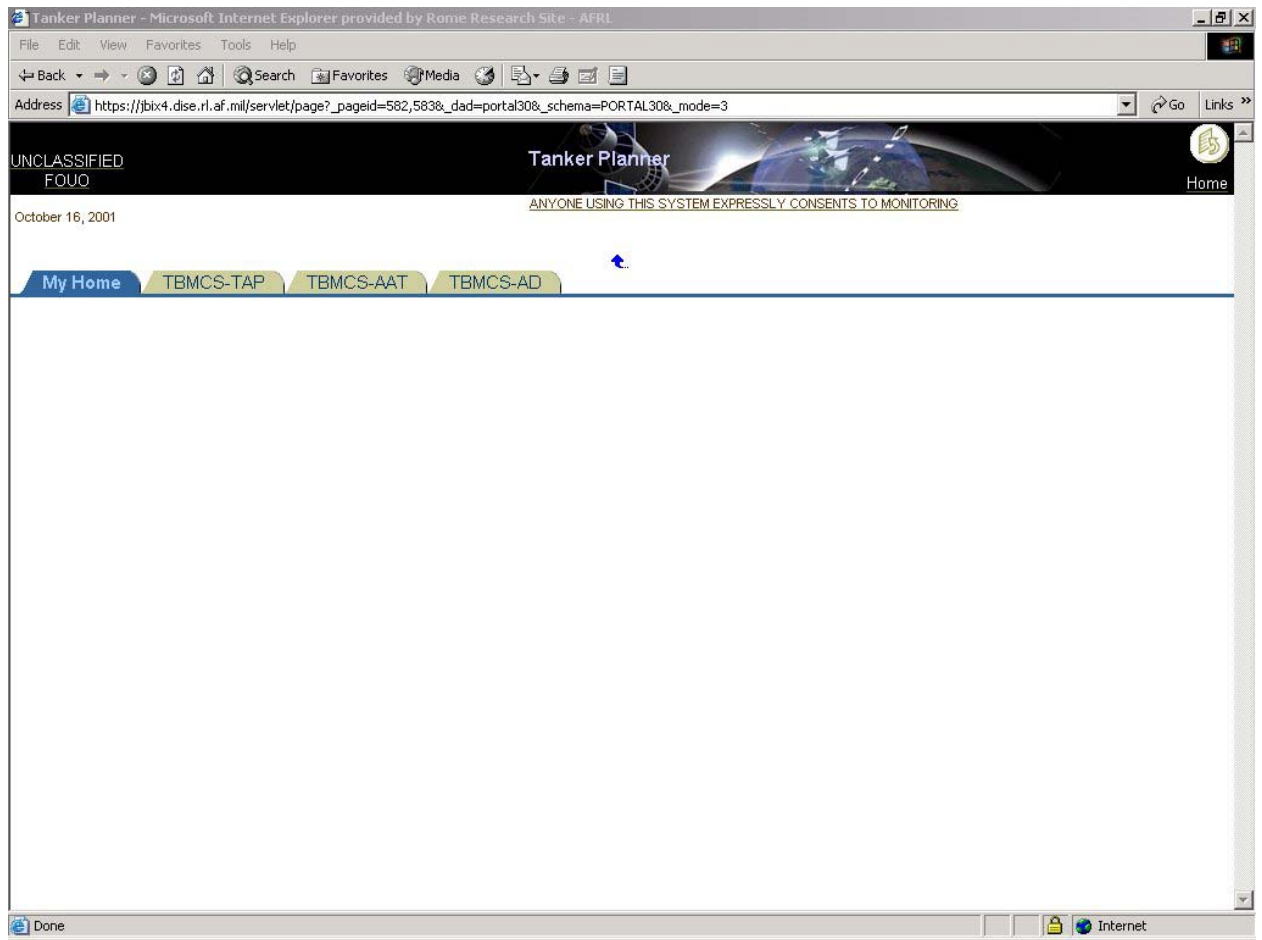


Figure B-13 Tanker Planner

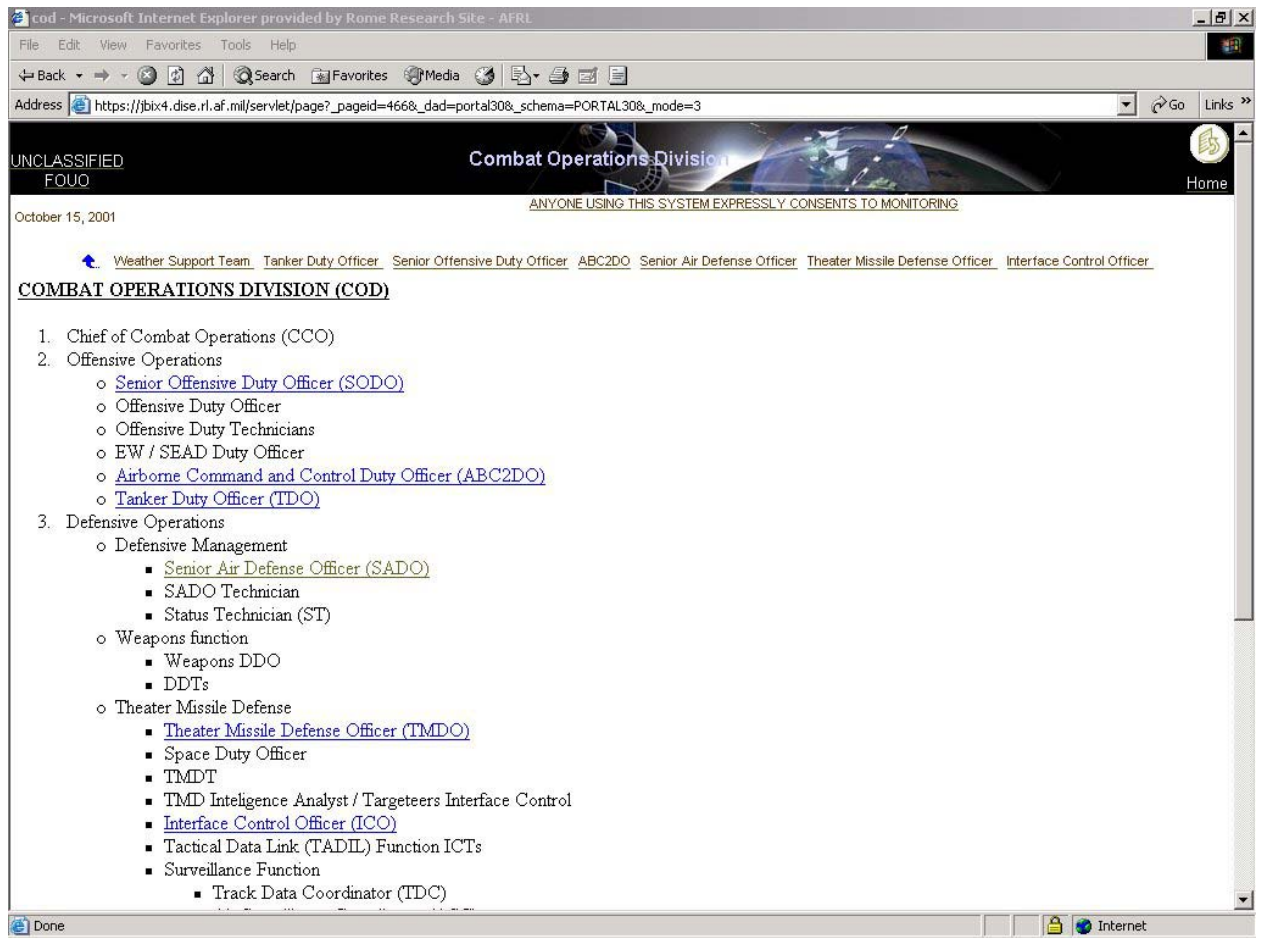


Figure B-14 Combat Operations Division

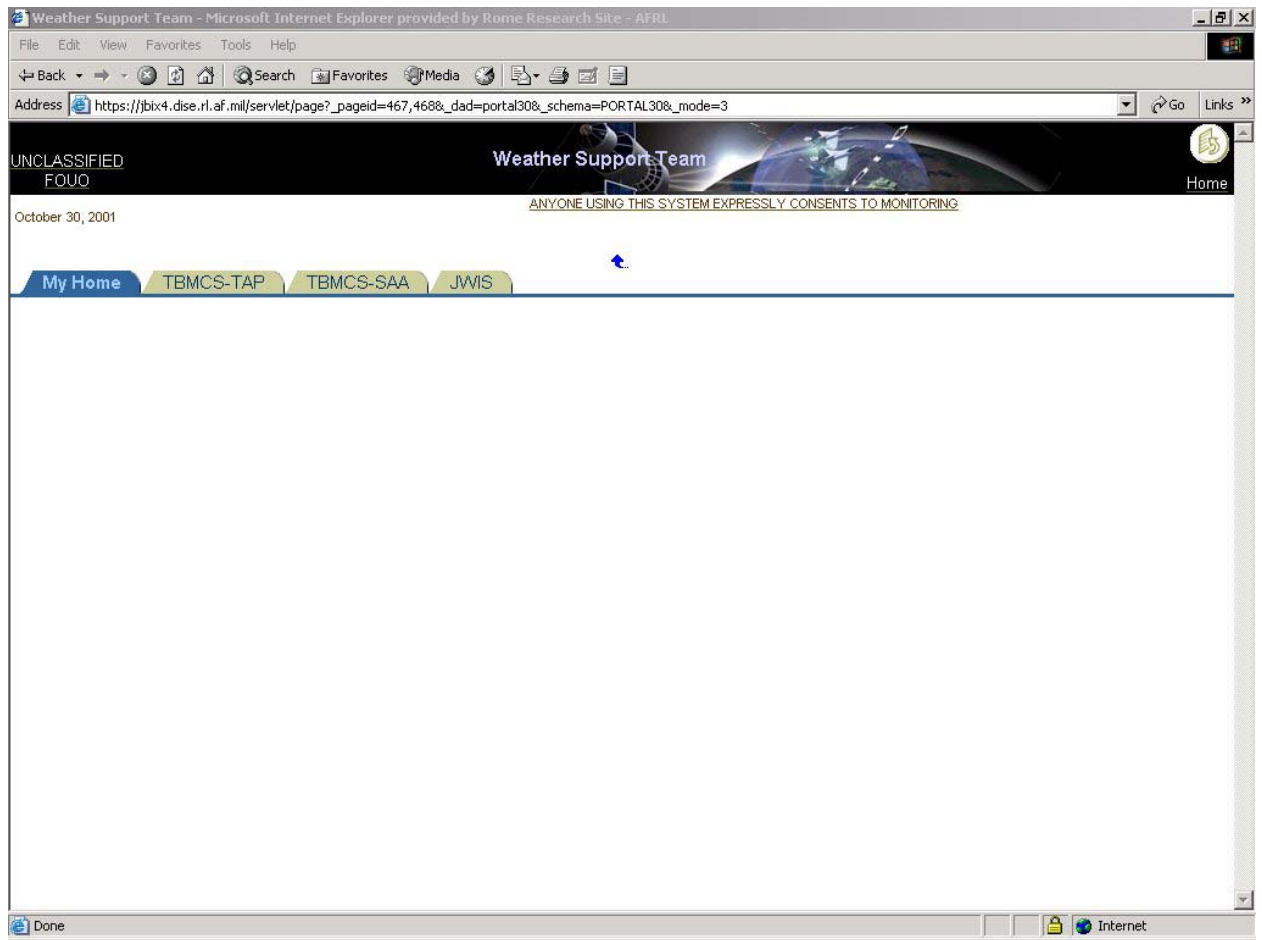


Figure B-15 Weather Support Team

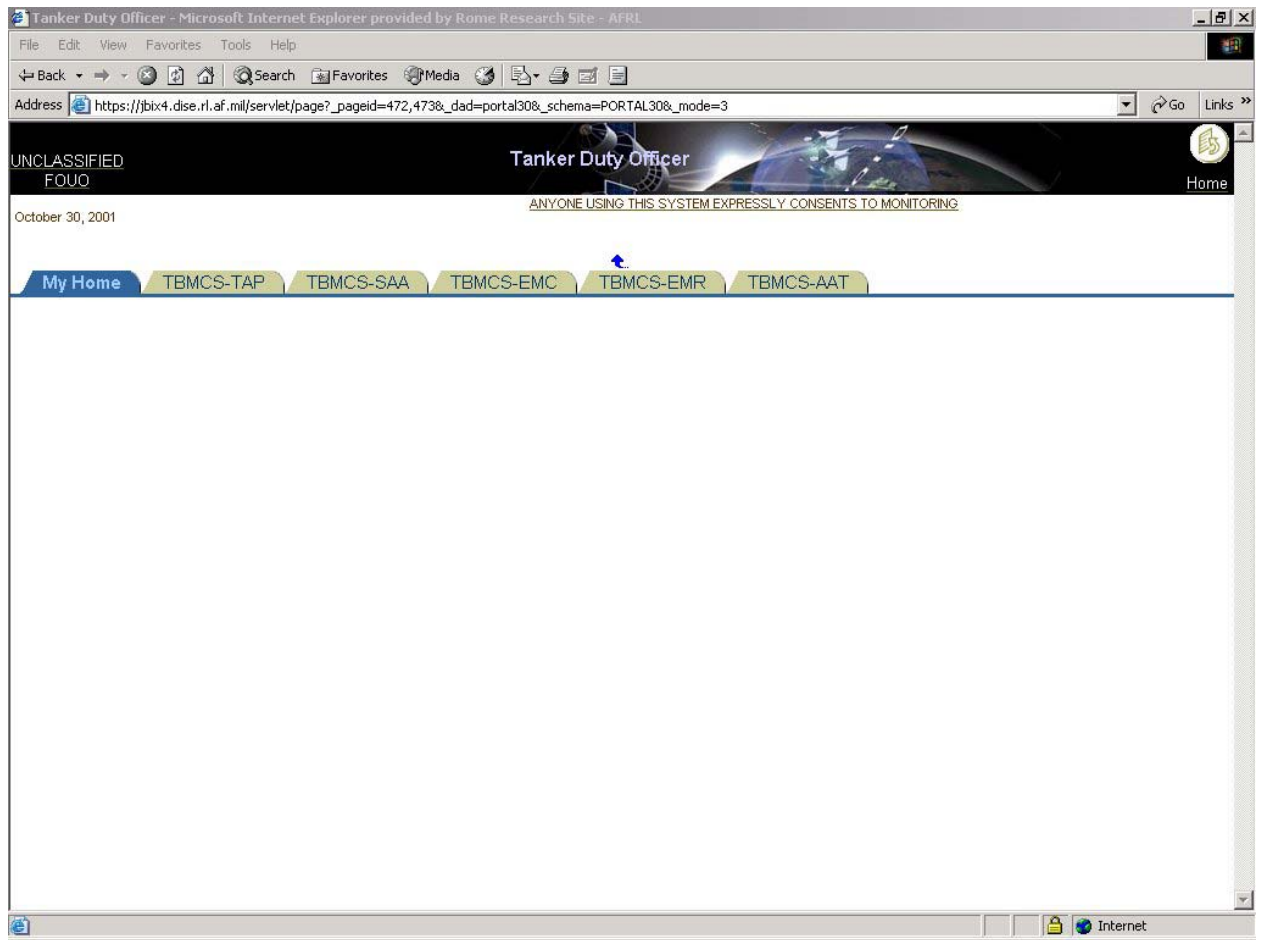


Figure B-16 Tanker Duty Officer

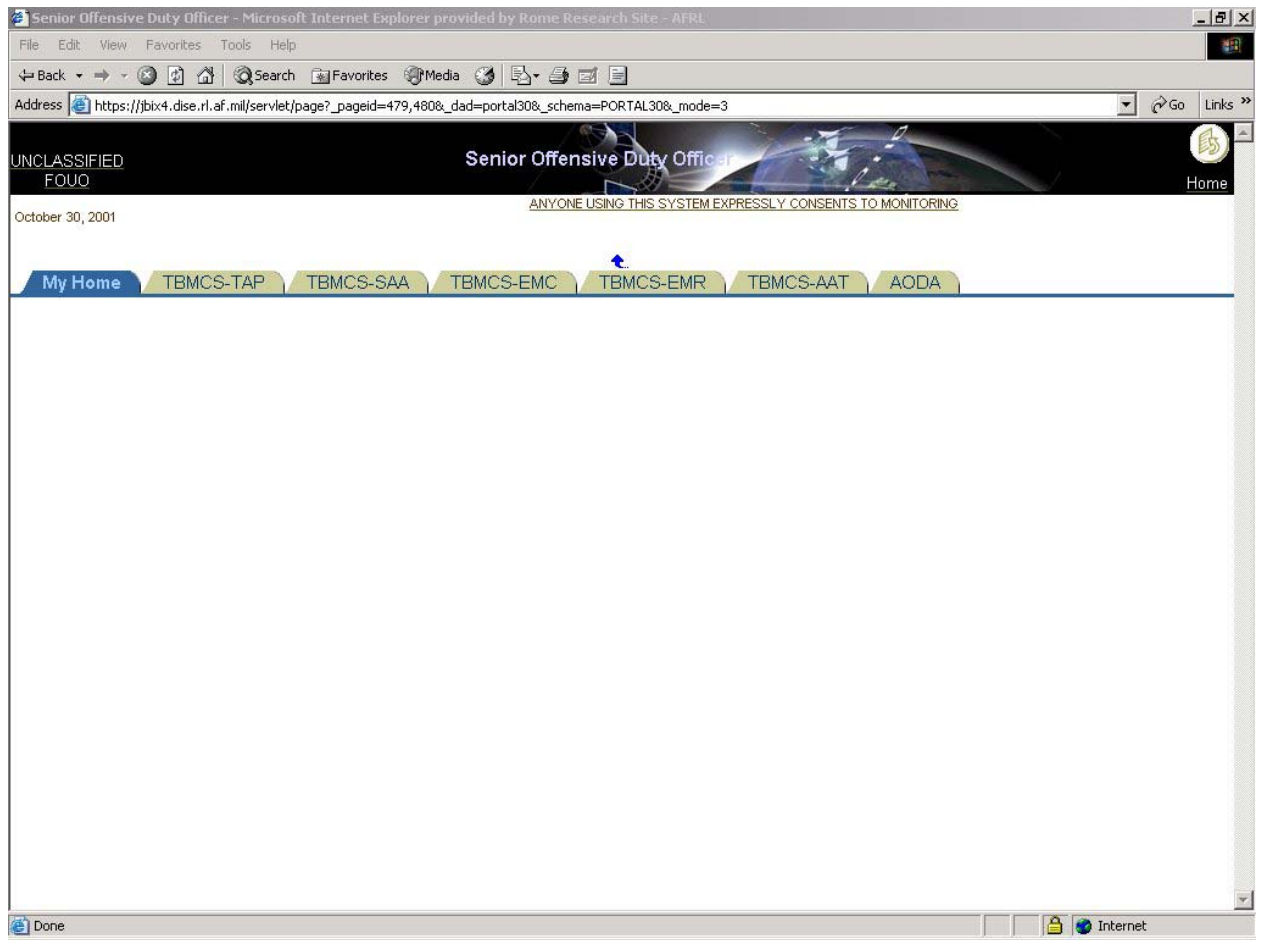


Figure B-17 Senior Offensive Duty Officer

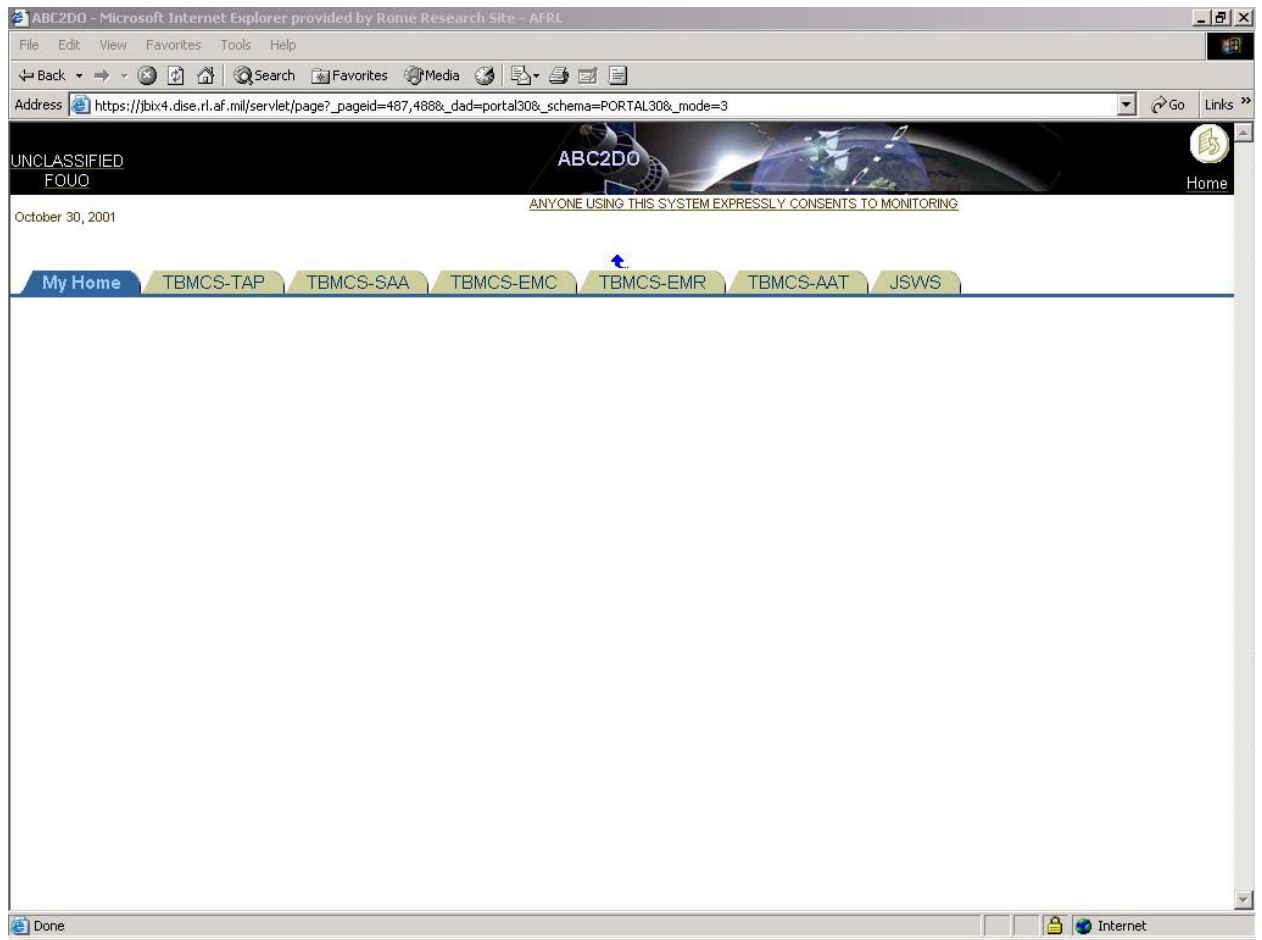


Figure B-18 ABC2DO

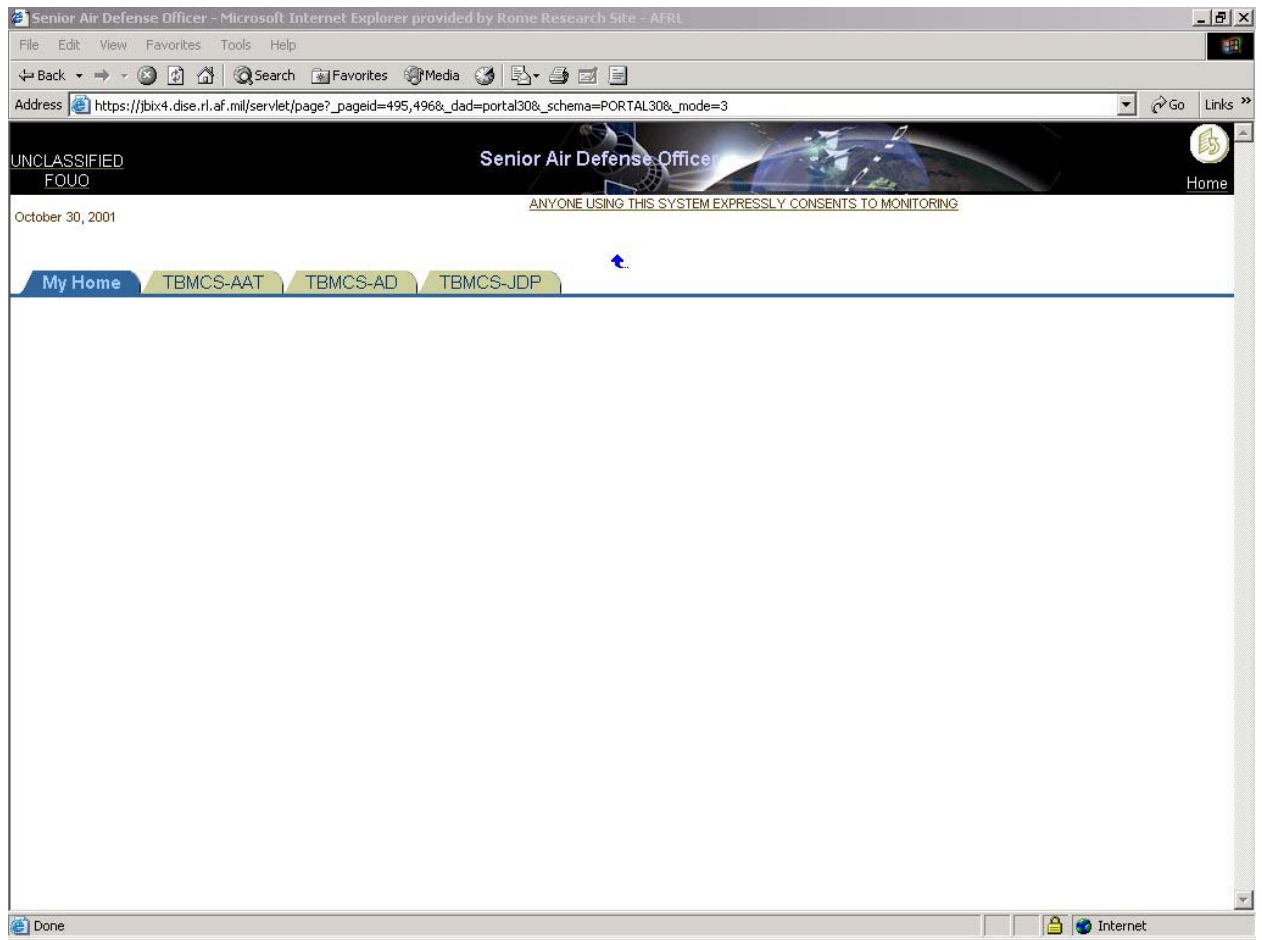


Figure B-19 Senior Air Defense Officer

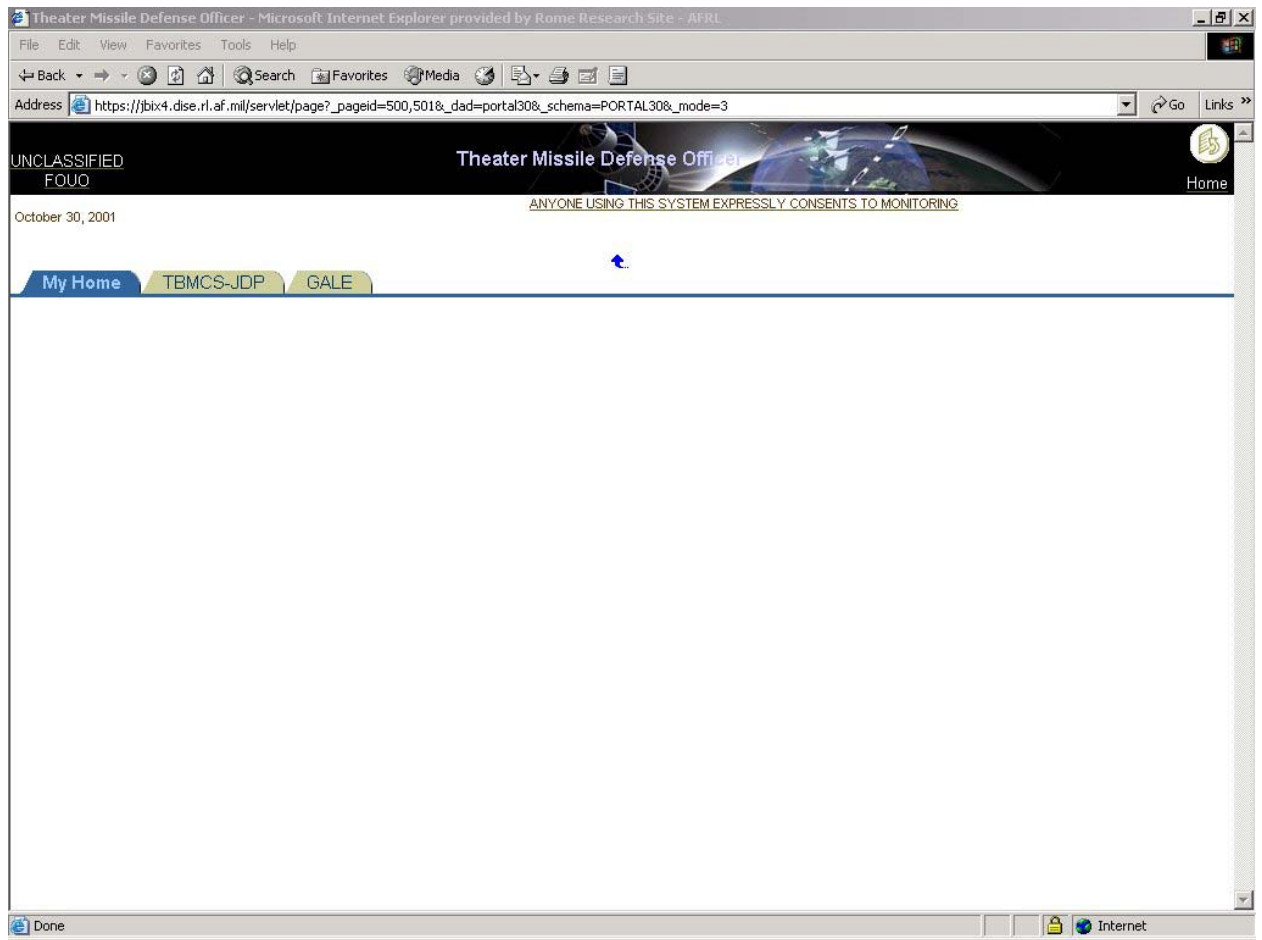


Figure B-20 Theater Missile Defense Officer

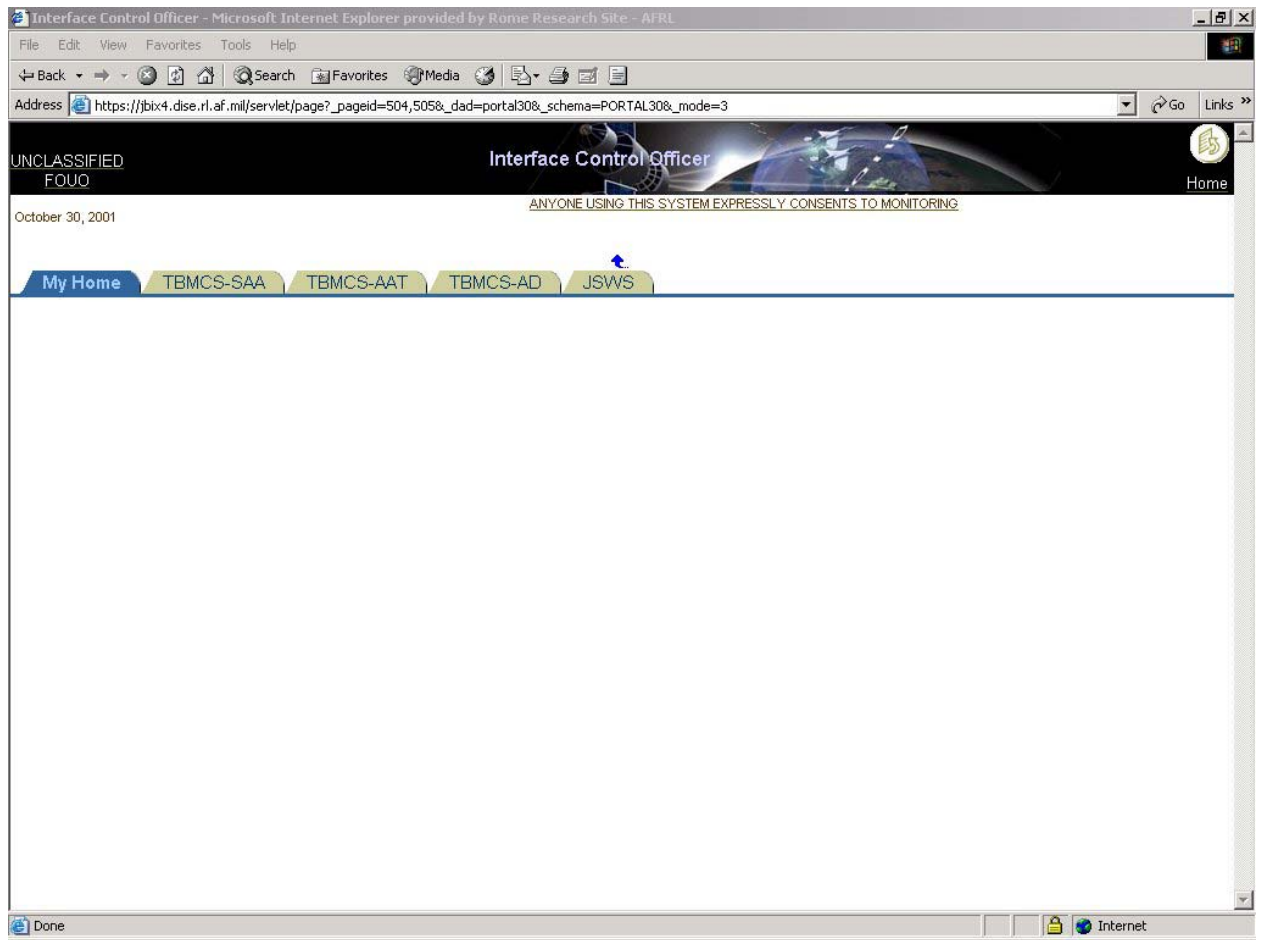


Figure B-21 Interface Control Officer

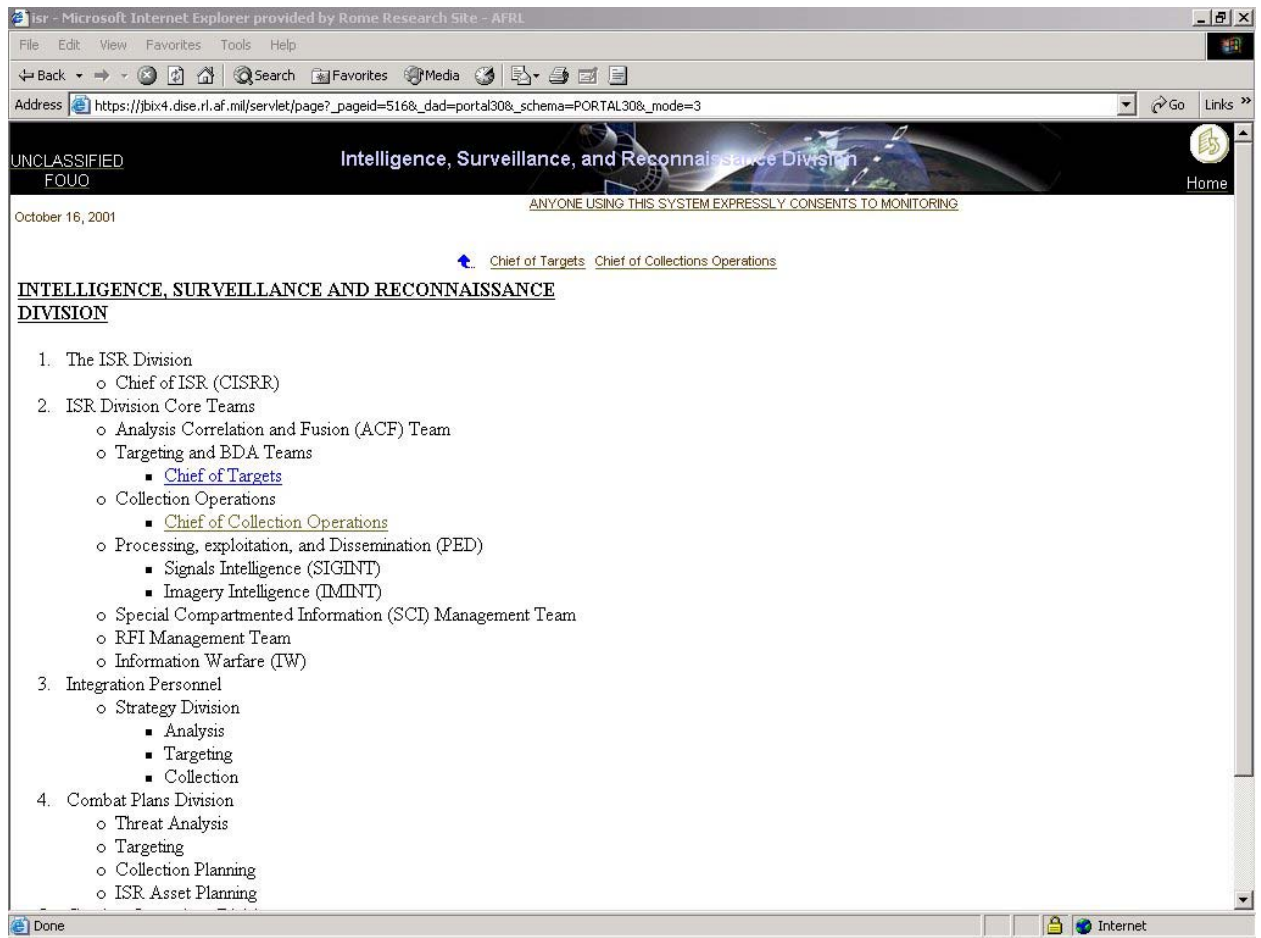


Figure B-22 Intelligence, Surveillance and Reconnaissance Division

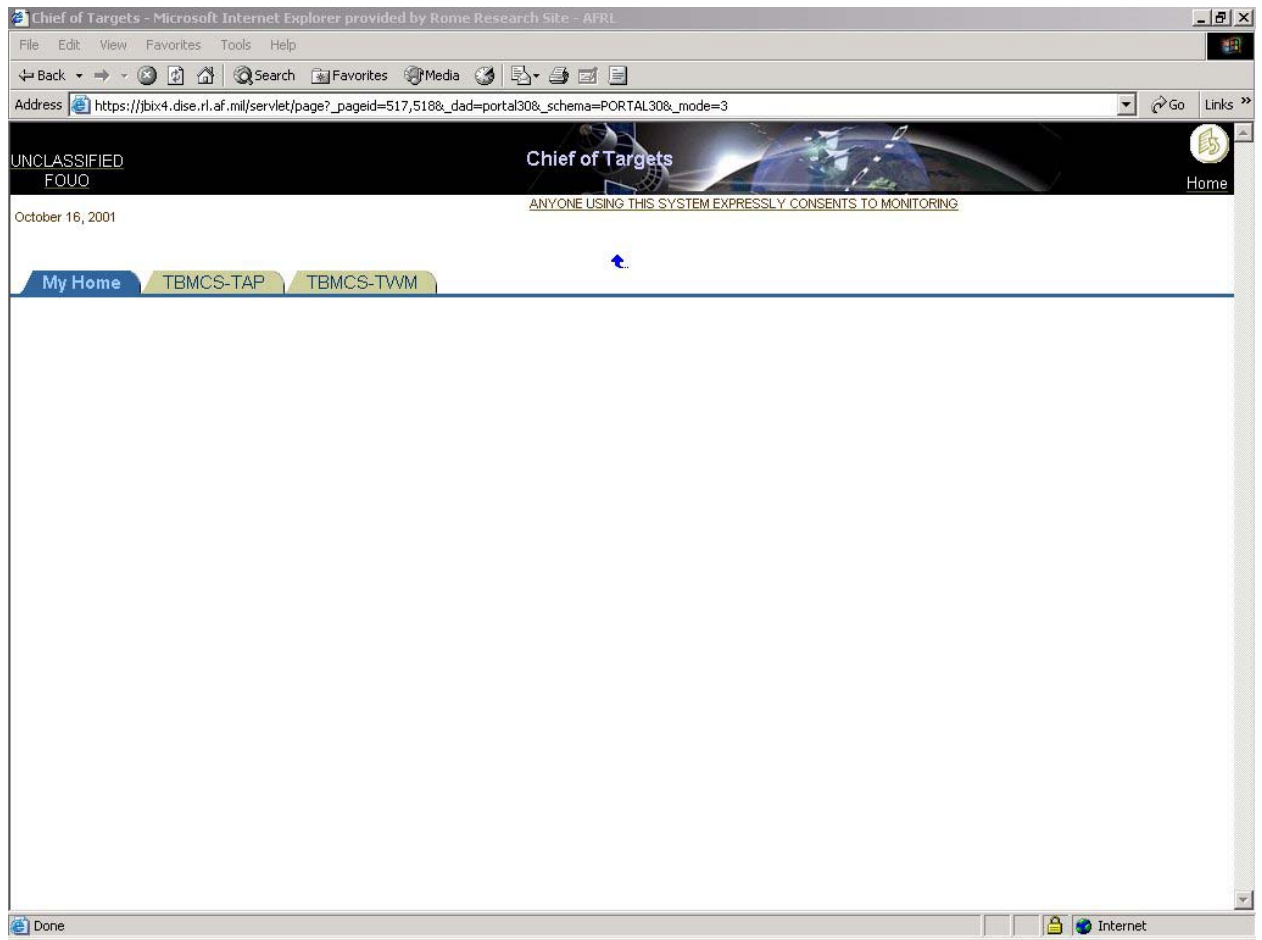


Figure B-23 Chief of Targets

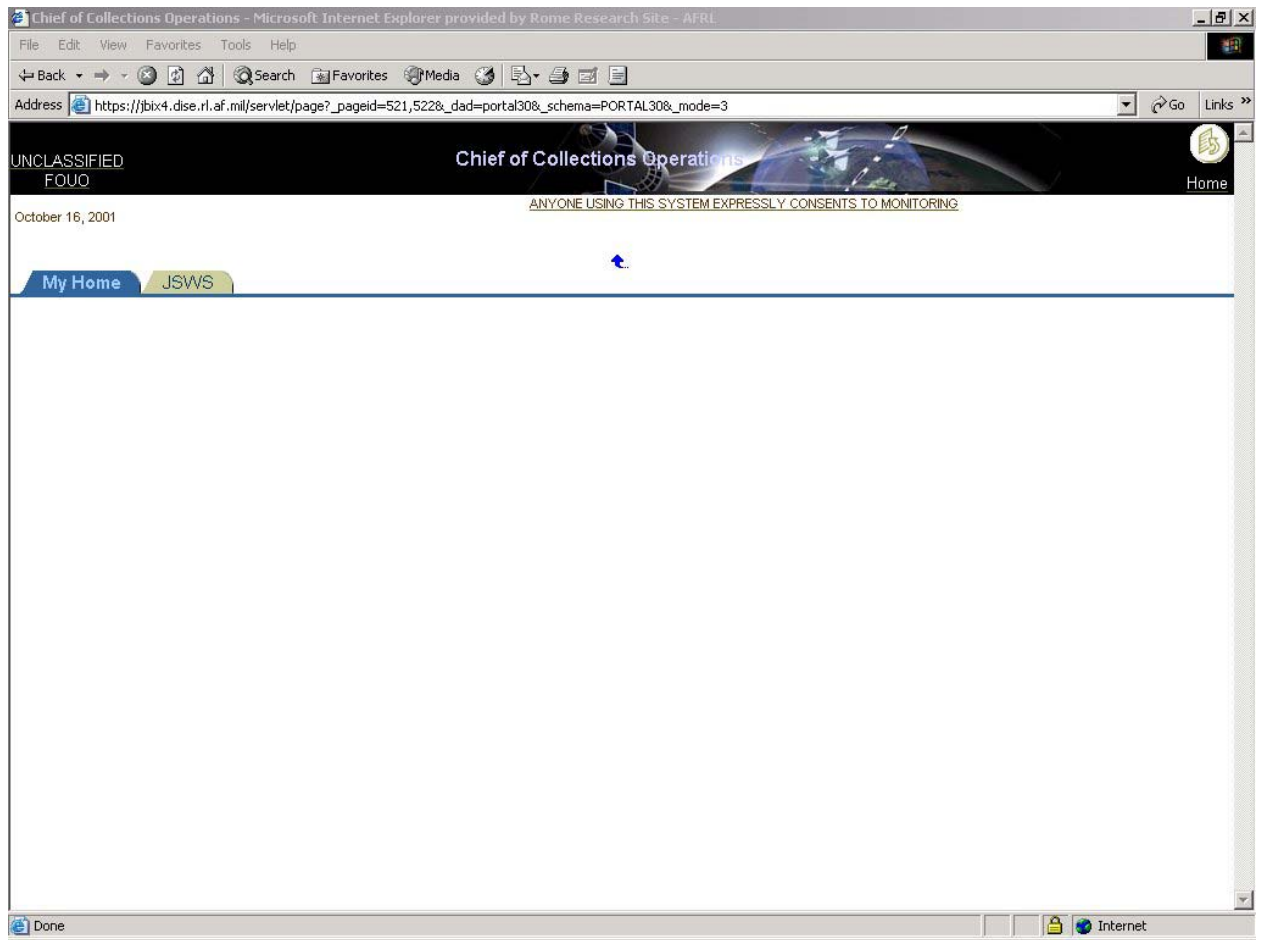


Figure B-24 Chief of Collections Operations

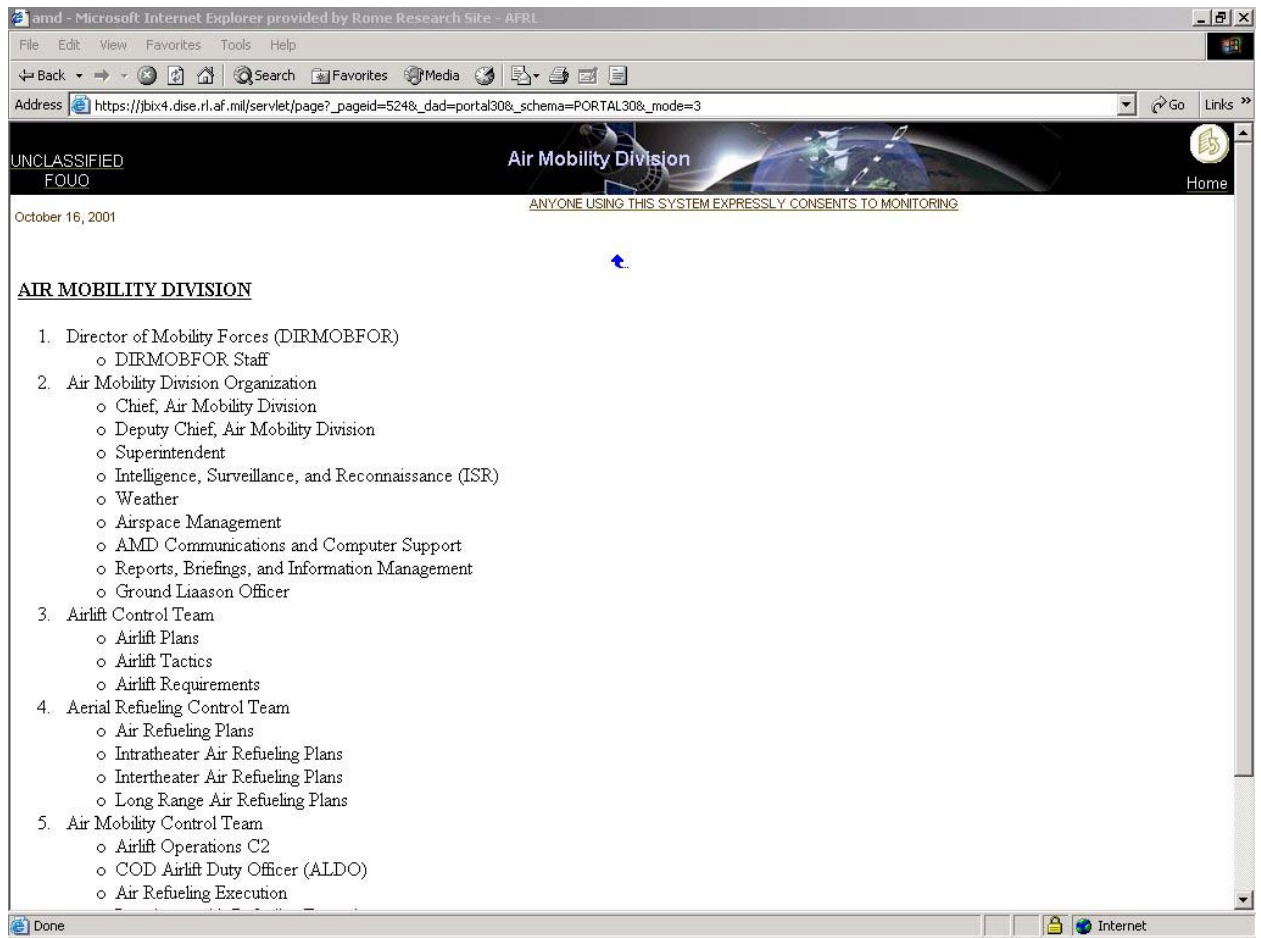


Figure B-25 Air Mobility Division

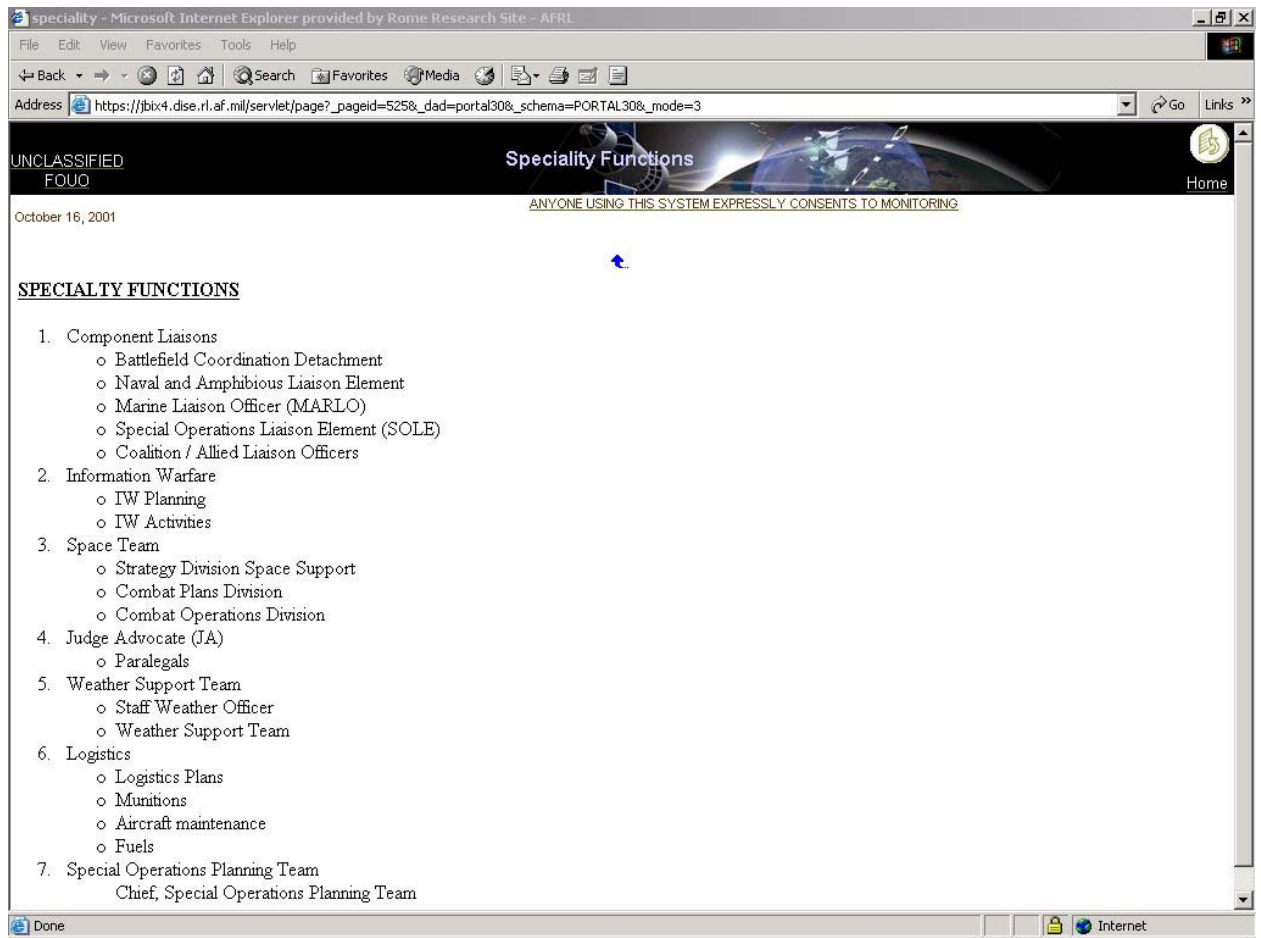


Figure B-26 Specialty Functions

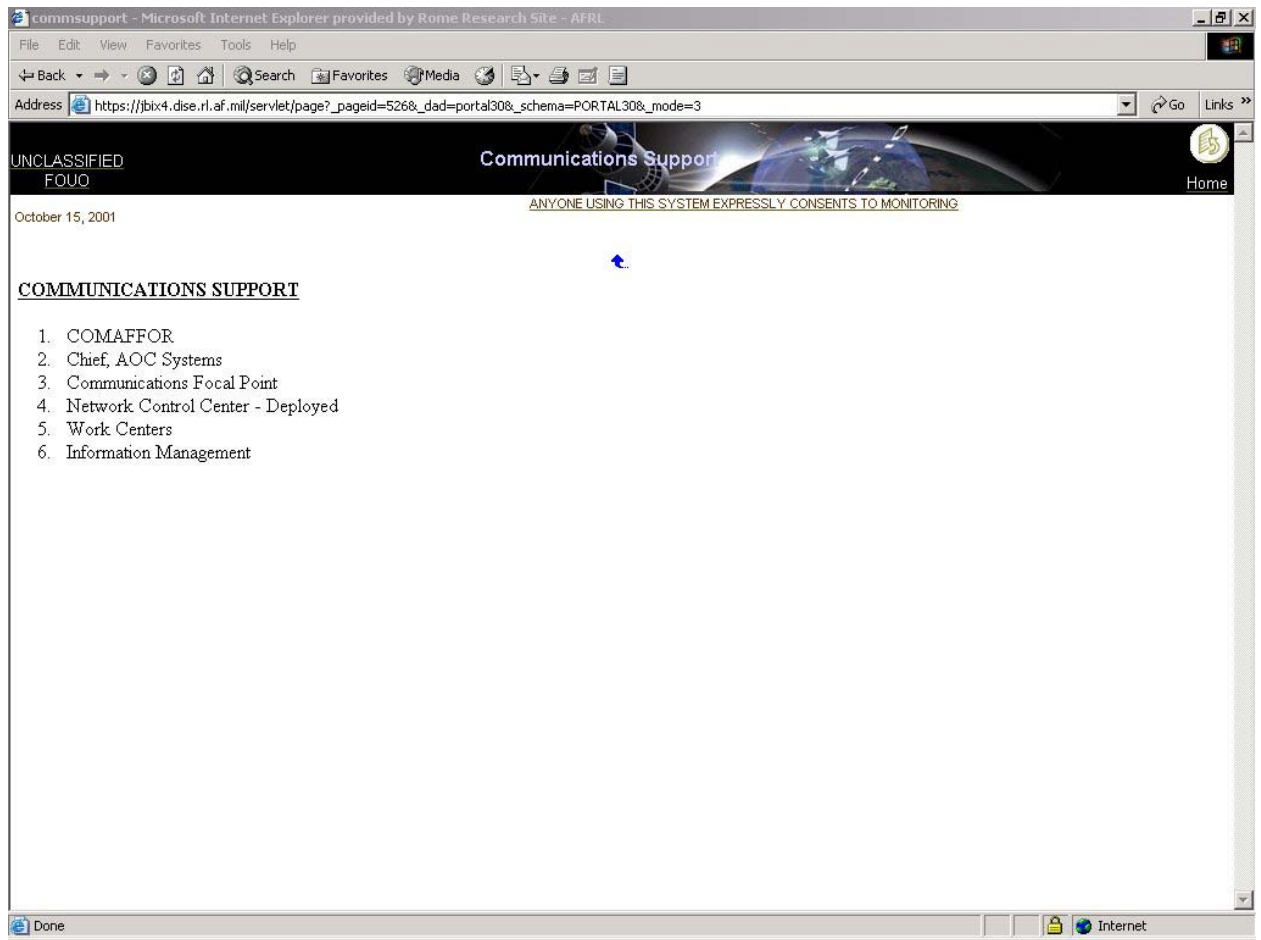


Figure B-27 Communications Support

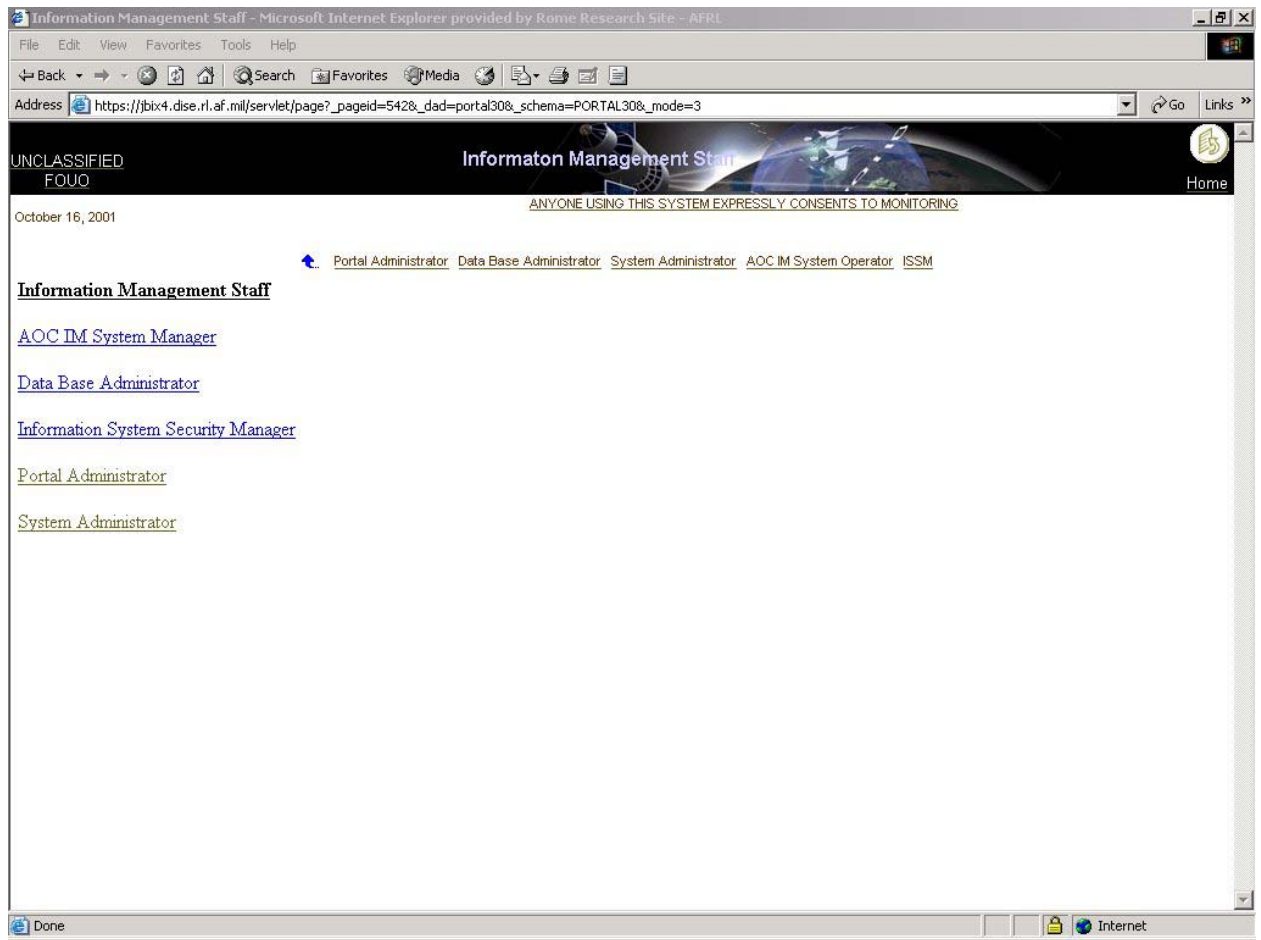


Figure B-28 Information Management Staff

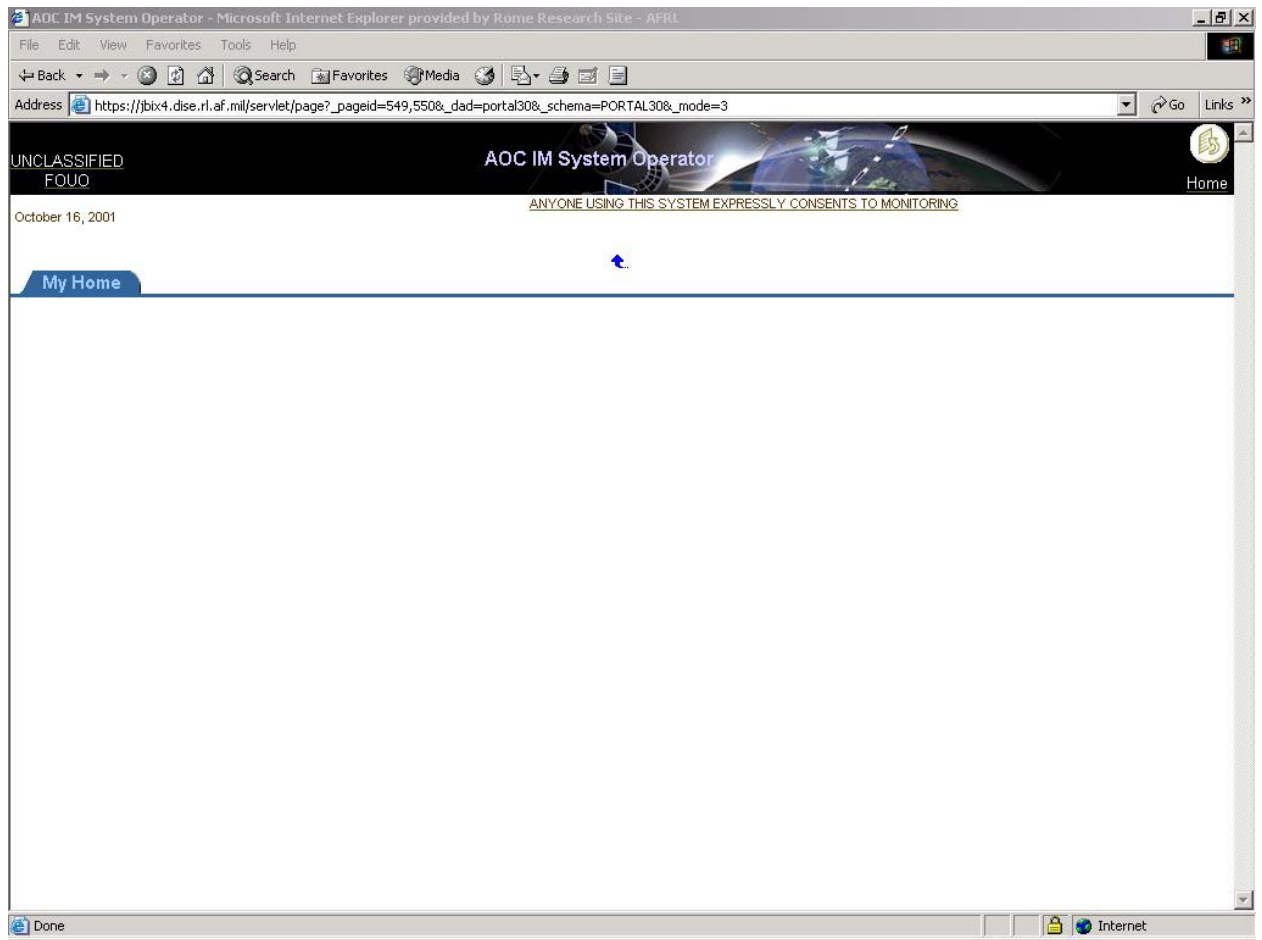


Figure B-29 AOC IM System Operator

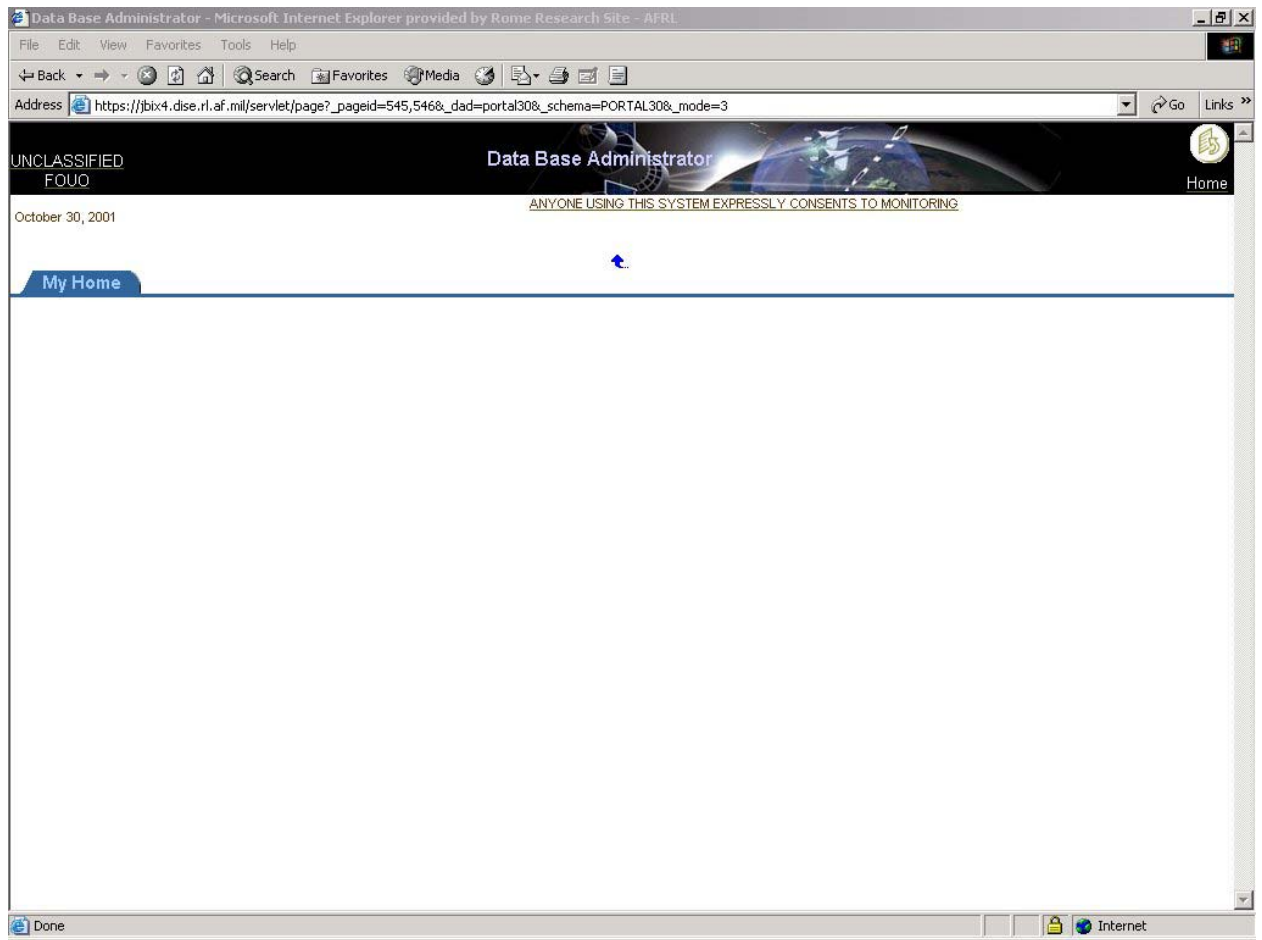


Figure B-30 Data Base Administrator

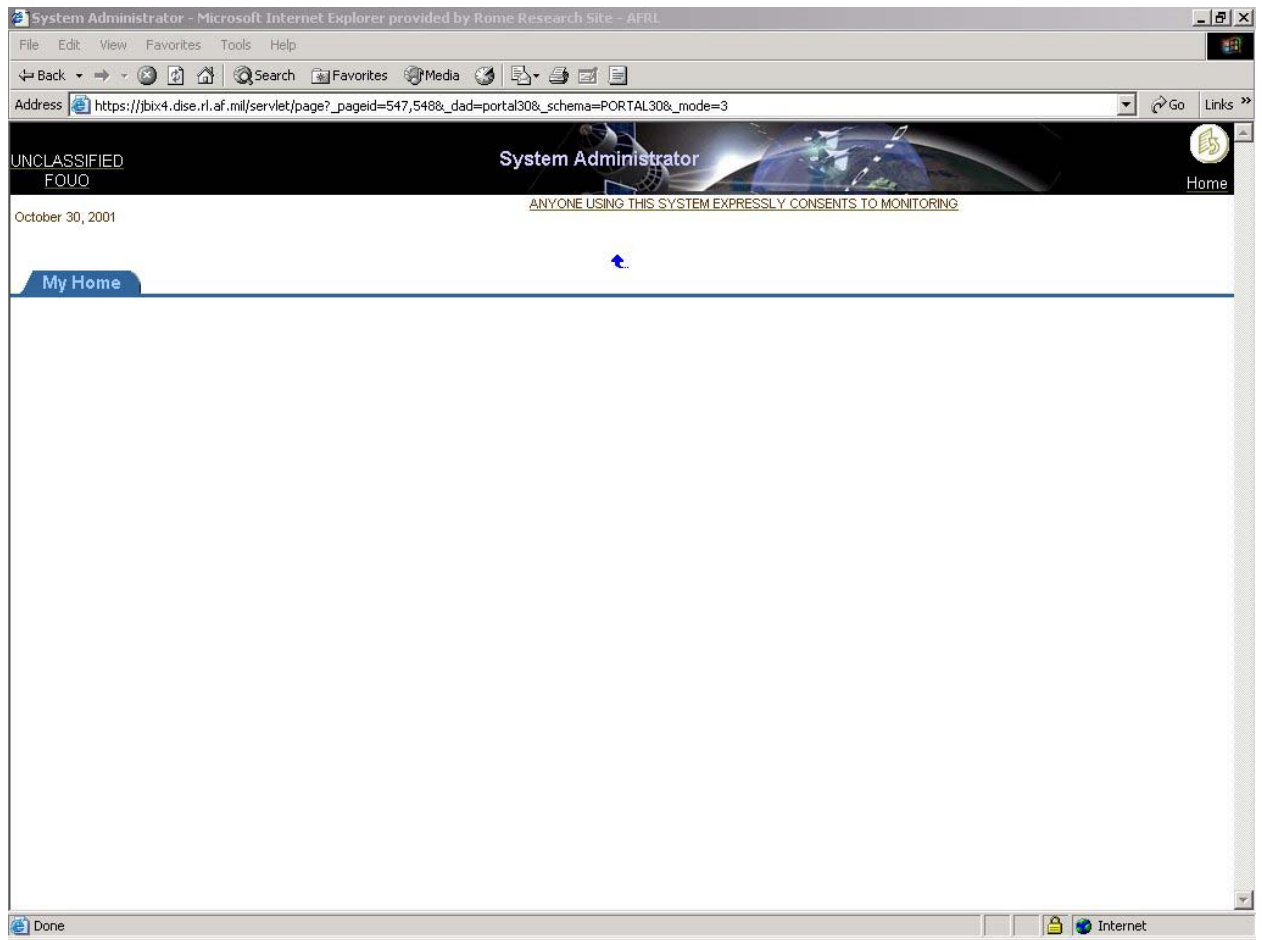


Figure B-31 System Administrator

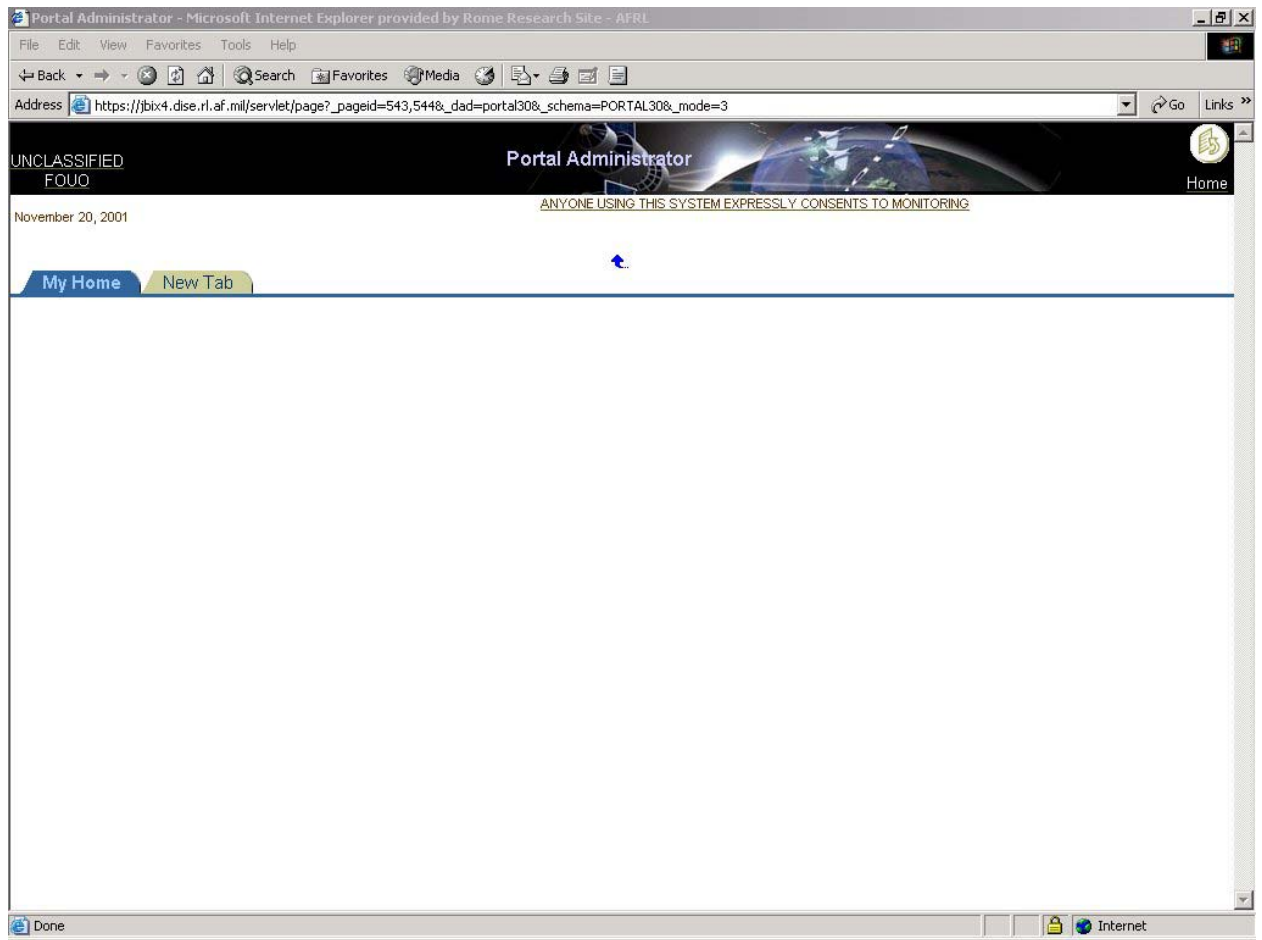


Figure B-32 Portal Administrator

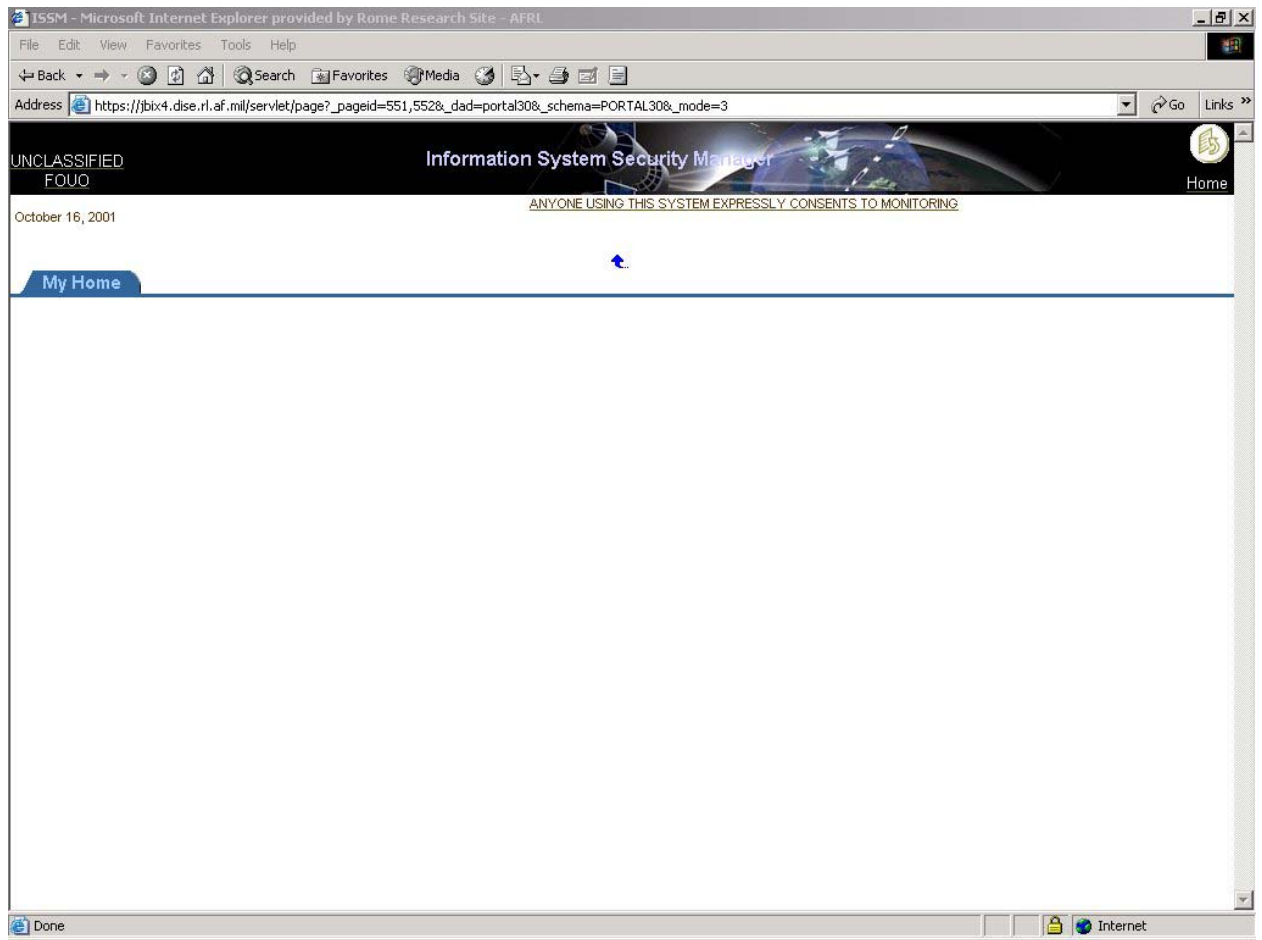


Figure B-33 Information System Security Manager

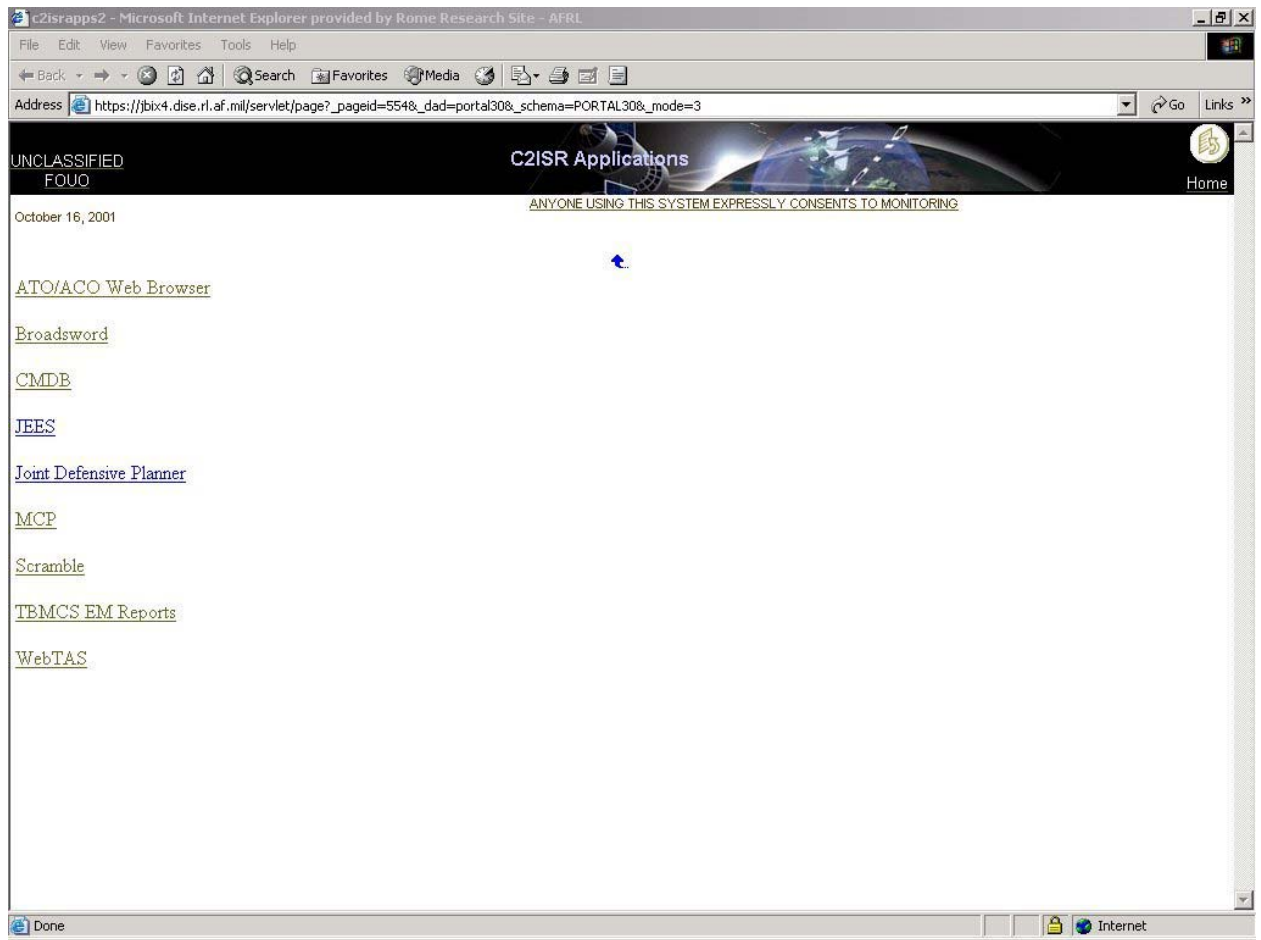


Figure B-34 C2ISR Applications

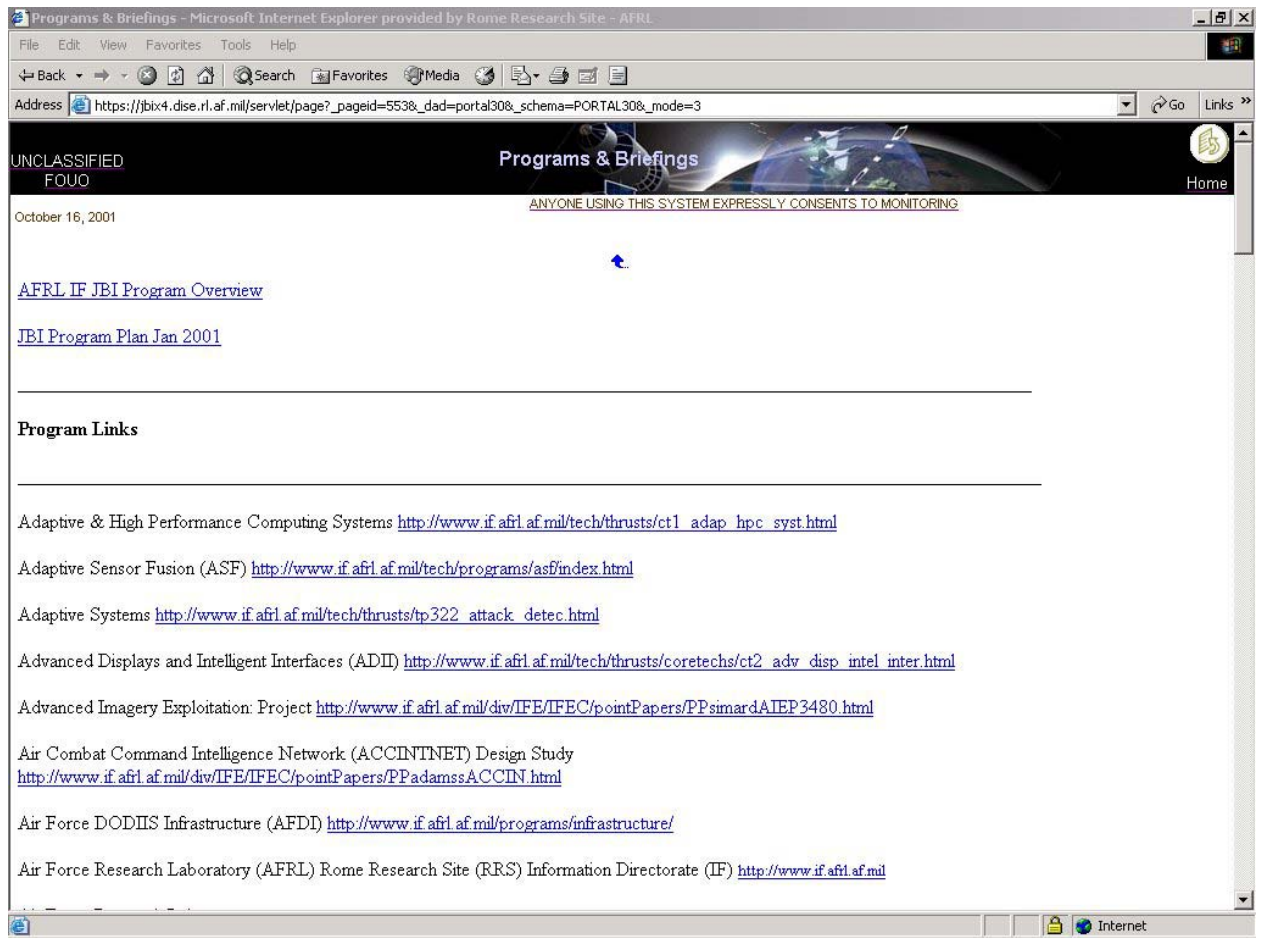


Figure B-35 Programs and Briefings

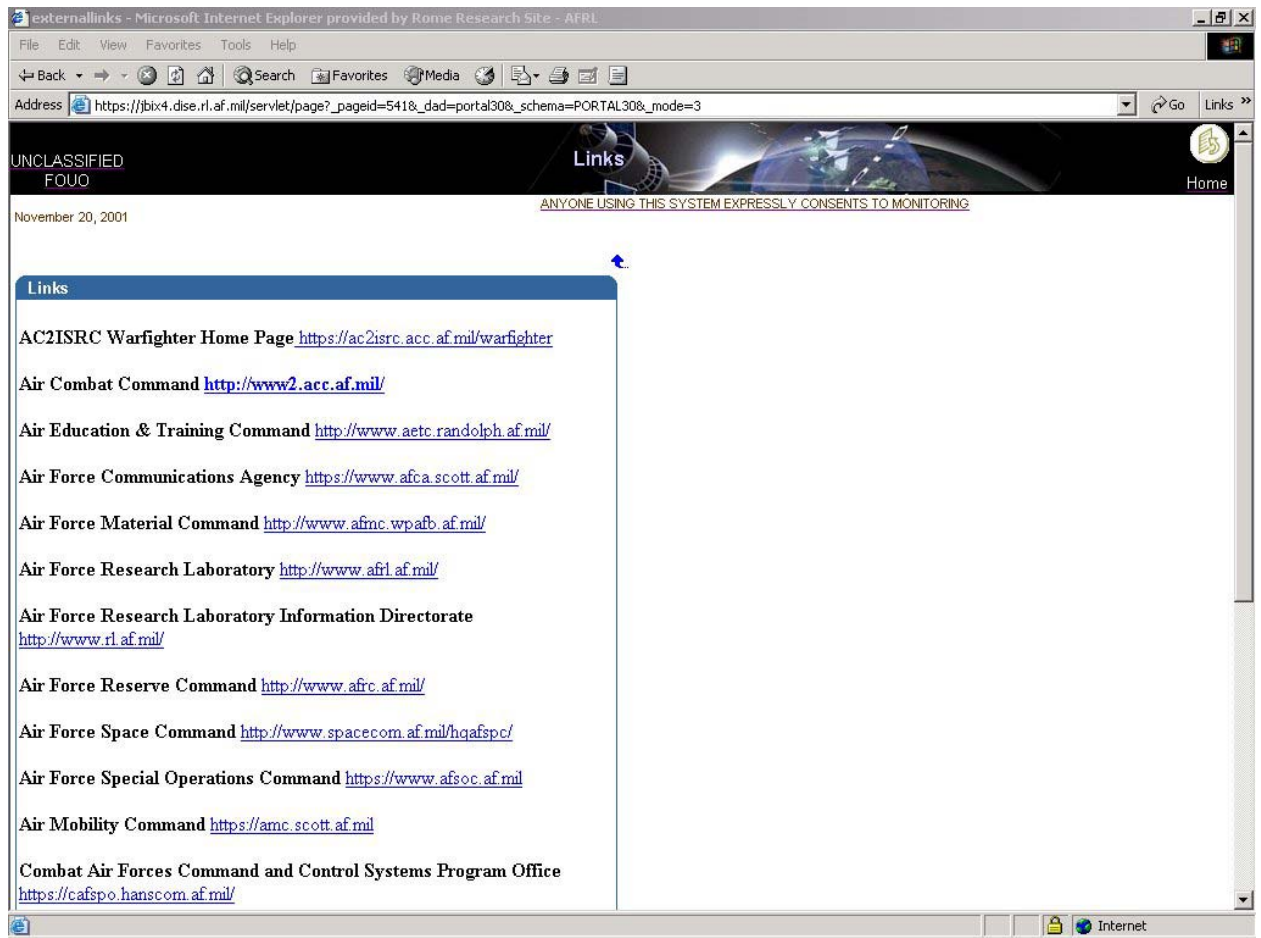


Figure B-36 Links

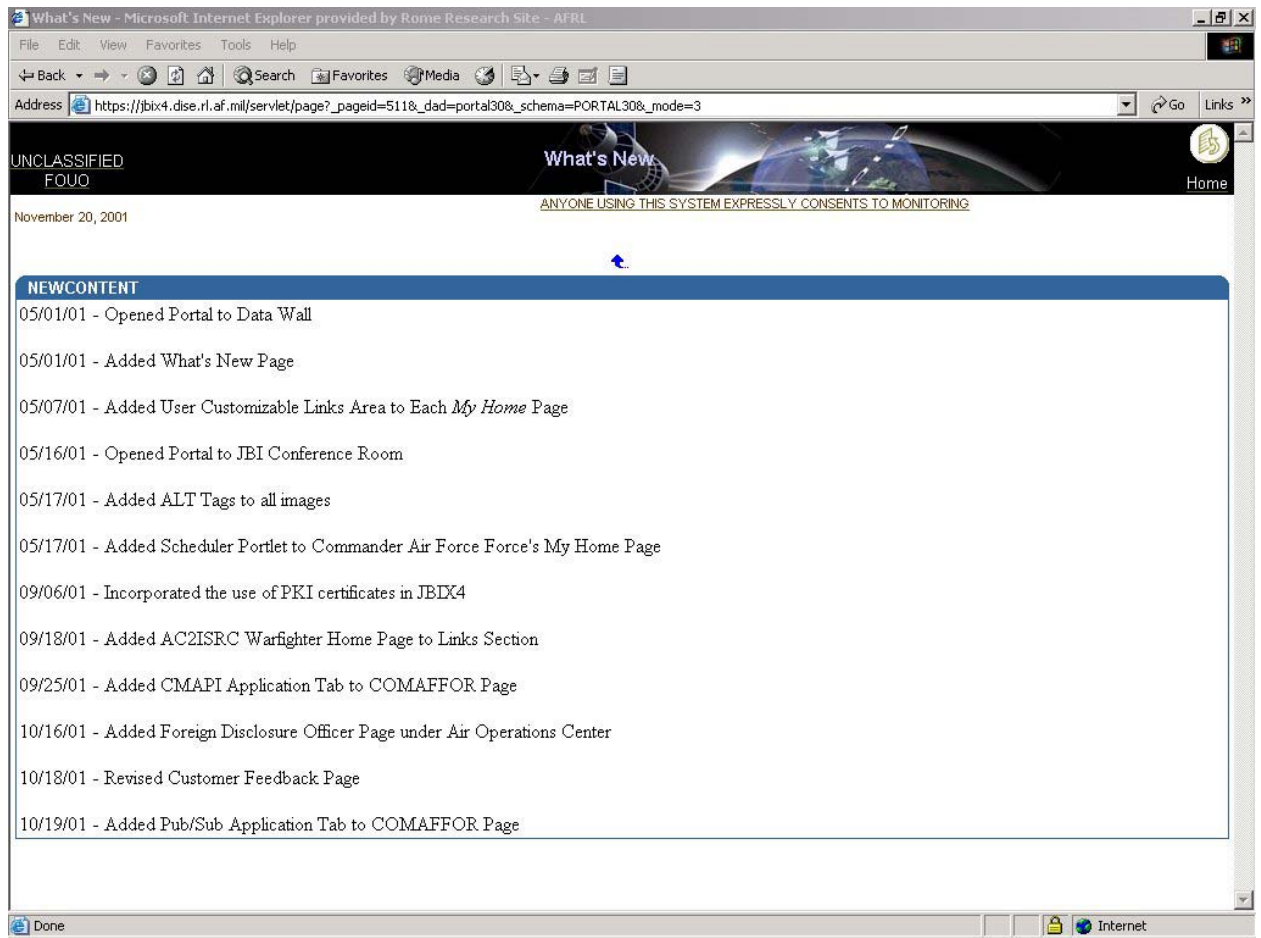


Figure B-37 What's New

Appendix C Chronology of Accomplishments Under TO-03 of JBI-DT Contract

This section presents a weekly log of the accomplishments/activities.

January 24, 2001

- Set up the Compaq hardware

January 31, 2001

- Set up the 2nd Compaq and placed all components under configuration control

February 9, 2001

- Loaded Solaris 7 and Netscape on jbix3.
- Secured jbix3 by applying RRS/IFOS Security Checklist
- Applied February 01 Patch Cluster to jbix3. This cluster appears to break the volume management daemon.
- Loaded Windows 2000 Advanced Server on jbix1 and jbix4
- Loaded Solaris 7 multiple times on JBIX0. The system does not boot off of internal hard disks. Still investigating.

March 15, 2001

- Assembled a book containing all of the CM information developed to date for jbix0 and jbix3 to include:
 - Hardware Inventories
 - Portal Startup/Shutdown Procedures
 - Address/System Information
 - Installation Notes
- Installed Miscellaneous Software on jbix0
- Installed Portal Tutorial on jbix0. Began working through it.
- Secured portal on jbix3.
- Assisted with the install of Oracle 9i on jbix0.

March 22, 2001

- Performed Level 0 dumps on jbix0 and jbix3
- Reloaded Windows 2000 on jbix1 and jbix4. Configured the external disk array on each as RAID 5 striped.
- Continued setting up the Portal Framework on jbix3.

- Gave a brief demo to two members of the British Military. They are trying to solve the same problem of providing web access to their applications and data and at the same time restricting access to only those that need it.

March 29, 2001

- Performed level 5 dumps on jbix0 and jbix3
- Continued configuring Portal Framework
- Redesigned JBIX Applications Page

April 5, 2001

- Performed Level 0 dumps on jbix0, jbix3
- Continued working on Portal Framework
 - Configured roles per AOC Regulation 13-1
 - Made several design changes to remove security "holes" (i.e. Made it harder for users to access parts of the portal that we don't want them to access)
- Established a method of allocating page access based on user authentication.

April 13, 2001

- Continued working on Portal Framework
 - Figured out how to load content such as files, JavaScript, apps, images, etc into Portal
 - Converted most of the existing html into portlets. Portlets are in effect objects that can be reused. This establishes a framework for future work.
 - Added new TBMCS images to the portal

April 19, 2001

- Performed Level 5 Dump of jbix0 and jbix3
- Oracle upgraded the portal software from 3.0665 to 3.08. Unfortunately the portal data base schemas between the two versions have changed significantly. To compound matters further, there are no migration scripts available between the two versions. As a result, the portal must be rebuilt. We could reinstall the previous version and reload the portal as is, however, we need some of the new features in the current portal version in order to be able to stand the portal up to either the public or rl.af.mil

April 26, 2001

- Performed Level 5 Dumps of jbix0, jbix3
- Rebuilt the portal taking advantage of Oracle's capability to generate dynamic HTML. By using dynamic HTML, we avoid several of the security concerns by using regular Oracle portlets.

May 3, 2001

- Performed Level 5 Dumps
- Continued routine development on the Portal
- Allowed additional access to portal to a couple of machines attached to different data walls.

May 10, 2001

- Performed Level 0 dumps of jbix0, jbix3.
- Added a What's New section and an Information Management Staff section to the Portal
- Began investigating the issues of system audits and allowing portal users to change their own passwords

May 17, 2001

- Level 5 Backups of jbix0 and jbix3
- Granted Portal Access to JBI Conference Room
- Reviewed numerous discussion groups and Frequently Asked Question lists on Portal
- Installed Portal Development Kit - necessary to install future portlets
- Configured two sample roles (one for a Portal Administrator and one for a Registered User). The Portal Administrator can pick and choose from six statistical/audit type portlets. The registered user can pick and choose from 9 C2ISR applications

May 23, 2001

- Performed Level 5 dumps of jbix0 and jbix3
- Attached <ALT> tags to all portal images
- Continued working with May PDK. It turns out to be buggy -- awaiting the June release.

June 7, 2001

- Performed Level 0 dumps of jbix0 and jbix3
- Used Oracle's report capability and created a report for all users who enter feedback in the User Feedback Portlet

June 14, 2001

- Created an Oracle Form which allows a privileged user to review and delete User Feedback records from the Portal
- Installed the latest URL Services extensions to the JPDK

June 21, 2001

- Level 5 Dumps of jbix0 and jbix3
- Continued working with the URL Services Portlet
- Began migrating the portal to jbix4 on the Compaq 8500
 - Reloaded the OS on the Compaq
 - Began exporting all of the portal components on jbix3 so they can be imported on jbix4

August 1, 2001

- Performed level 0 dumps of jbix0 and jbix3
- Continued migrating portal to jbix4 by installing the java portlet development kit (JPDK) and the URL Services portlets. Still need to install the calendar and custom feedback portlets.

August 8, 2001

- Performed a level 5 dump of jbix0 and jbix3.
- Continued migrating portal to jbix4 by installing the Customer Feedback Portlet, a Monthly Calendar Portlet and the Scheduler Portlet. The only function remaining is the installation of user self-registration .

August 15, 2001

- Performed Level 5 Dumps on jbix3 and jbix4
- Installed and configured the self-registration portlet on jbix4. That completes the portal installation. Tested all of the links and portlets on jbix4 to verify their operation.
- Installed an Oracle patch on jbix3 that corrected a security vulnerability with the listener.
- Began scoping the task to convert the portals to https.

August 22, 2001

- Requested DoD PKI Server Certificate for jbix4

August 29, 2001

- Obtained PKI Certificate and began configuring jbix4 to use https.
- Tried to install IAS and Portal on jbix1 (Windows 2000 machine). The install interfered with the Jumpstart Application that we had already installed on jbix1. Uninstalled IAS/Portal and fixed Jumpstart.
- Began investigating how to export "All" of the portal content from jbix1 to jbix4. The export from JBIX3 to JBIX4 required reinstallation of several components and a significant amount of manual configuration.

September 5, 2001

- Worked on configuring jbix4 to use Government PKI certificates. The bjix4 recognizes the https request will not correctly render the servlets (ie. display content). Filed posts to Oracle's Technet and Metalink and emailed Oracle. This problem must be solves in order to start building the SIPRNET Portals.
- Performed Level 0 dumps of jbix0, jbix3.

September 12, 2001

- Successfully configured jbix4 to work with Government issued PKI certificates.
- Began taking a series of classes necessary to get SIPRNET account.
- Performed Level 5 backups of jbix0 and jbix3

September 26, 2001

- Installed CMAPI on jbix4 and integrated it into the portal

October 3, 2001

- Added more CADRG data to CMAPI on jbix4 including Afghanistan
- Built another CMAPI application that allows the user to download the necessary browser java plug-in and it also provides a link to the CMAPI web site.
- Built a web page that tells the user how to configure the .java.policy file.

October 24, 2001

- Added links to jbix3/jbix4 for the Unclassified 24x7 Server
- On jbix4, modified the Customer Feedback Portlet to include the customer's email address; then linked the portlet to the homepage
- On jbix3 and jbix4, added application tabs for Homeland Defense pages.

October 31, 2001

- Experimented with Oracle's URL Services
- Found out this week that Oracle's redirection module does not handle https calls. Oracle provided a patch which was installed. This explains the unexplained errors on jbx4 occurring for a couple of months. Now that the JBI program has two functional portals. (jbx3, Solaris) and (jbx4, Windows 2000, https).
- Granted external hosts access to the portal.

Appendix D. Acronyms

ABC2DO	Airborne Command and Control Duty Officer
AC2ISRC	Aerospace Command, Control, Intelligence, Surveillance, and Reconnaissance Center
AFDI	Air Force DoDIIS Infrastructure
AFRL	Air Force Research Laboratory
AOC	Air Operations Center
ACO	Airspace Control Order
ATO	Air Tasking Order
C2	Command and Control
C2B	Command and Control Battlelab
C2IPS	Command and Control Information Processing System
C2ISR	Command and Control, Intelligence, Surveillance and Reconnaissance
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C2TC	Command and Control Technology Center
CAOC-X	Combined Air Operations Center-Experimental
CFACC	Combined Air Force Component Commander
CM	Configuration Management
CMAPI	Core Mapping Application Program Interface
CMDB	Configuration Management Database
COMAFFOR	Commander Air Force Forces
COTS	Commercial-Off-the-Shelf
CUBE	Command and Control Unified Battlespace Environment
DAD	Database Access Descriptor
DBA	Database Administrator
DBCC/TCTC	Dynamic Battle Control Center/Time Critical Targeting Cell
DCGS	Distributed Common Ground Systems
DFAS	Defense Financial and Accounting System
DII COE	Defense Information Infrastructure Common Operating Environment
DoD	Department of Defense

DoDIIS	Department of Defense Intelligence Information System
DT	Distributed Testbed
EM	Execution Management
ESC	Electronic Systems Command
GCCS	Global Command and Control System
GCCS-AF	Global Command and Control System-Air Force
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
HTTPS	Secure Hypertext Transport Protocol
IAS	Internet Application Server
IDIQ	Indefinite Delivery, Indefinite Quantity
IER	Information Exchange Requirements
IOC	Initial Operating Capability
IT	Information Technology
JB	Joint Battlespace Infosphere
JB-DT	Joint Battlespace Infosphere-Distributed Testbed
JBC	Joint C4ISR Battle Center
JEES	Joint Environment Exploitation Segment
JXP	JB Experimental Portal
MCP	Master Caution Panel
OSC	Operations Support Center
PDK	Portlet Development Kit
PKI	Public Key Infrastructure
PUB	Publication
R&D	Research and Development
RRS	Rome Research Site
SBMCS	Space Battle Manager Core Systems
SSL	Secure Socket Layer
SIPRNET	Secret Internet Protocol Router Network
SQL	Structured Query Language
SUB	Subscription
SWC	Space Warfare Center

TAR
TBMCS
TO

Technical Assistance Request
Theater Battle Management Core Systems
Task Order

URL
USAF
USAF IT
Technology
USJFCOM

Uniform Resource Locator
United States Air Force
United States Air Force Information

United States Joint Forces Command

WebTAS
wfJBI

Web Enabled Timeline Analysis System
Wright Flyer Joint Battlespace Infosphere

Appendix E Oracle 9i Press Release

AFRL-R 01-75

Air Force Research Successfully Completes Testing of Oracle9i Database

ROME, N.Y., Oct. xx, 2001 --- Air Force Research Laboratory engineers have successfully completed participation in a six-month test program for the next-generation database and internet server being developed by the Oracle Corporation. Evaluation of technology focusing on networked database security was the primary goal of participation in Oracle's "Beta Test Program for Version 9i."

Under the auspices of its Joint Battlespace Infosphere (JBI) program, the AFRL Information Directorate focused its efforts on ensuring the latest major release of Oracle software adheres to stringent Air Force and Department of Defense guidelines for security of data generated and stored in mission-critical command and control, intelligence, surveillance and reconnaissance (C2ISR) information systems. Security issues remain a high priority as Air Force C2ISR legacy systems undergo re-engineering and a move towards using open commercial product-based architectures and standards that are based on the internet and World Wide Web. The Department of Defense has adopted internet-like technology to support command and control of worldwide military and humanitarian operations.

The directorate has numerous technology programs addressing information management issues, but the JBI is one of its flagship efforts. Originally described by the Air Force Scientific Advisory Board (SAB) in a 1998 report and refined a year later, the JBI is a combat information management system that provides individual users with the specific information required for their functional responsibilities during crisis or conflict.

The SAB is a committee that provides independent guidance and insight to Air Force senior leadership on science and technology for continued air and space dominance. One of the panel's main recommendations in its 1999 report was to "focus the AFRL, other Service research labs, and battlelabs on evaluating and applying commercial technologies for the JBI."

Participation in the Oracle 9i Beta effort was an implementation of the SAB's guidance to develop the JBI by evaluating and incorporating suitable commercial off-the-shelf (COTS) products. AFRL leveraged and extended its in-house expertise by applying for Oracle 9i Beta Test Site status in January. In its proposal, the directorate team identified security as the project focus area and generated stress tests and remediation plans. The directorate was selected in February as one of a small number of Oracle beta sites located world-wide. To

augment the existing team, AFRL brought on additional Oracle technical support from the company's Advanced Products Group (APG) Reston, Va. This joint participation between industry and government research and development teams strengthened deep-rooted technical ties dating back to the mid-1980's and the work accomplished in producing security-related or "trusted" database products.

"Oracle has a rich history of working closely with Air Force engineers on leading edge C2ISR programs such as the JBI," said William Maimone, vice president, Server Platform Technology for Oracle. "This Beta test is an excellent example of real government/industry interaction on the COTS leading edge. The AFRL cadre and their beta test findings were both outstanding."

"Participating in the Oracle9i Database beta program gave us a great opportunity to continue our work with Oracle in the security area and influence future commercial product releases," said Charles Flynn, lead engineer from the Information Directorate. "Oracle is working to improve secure access to information and developing products which exhibit a lot of appeal to the military C2ISR systems designers."

"The JBI team provided excellent applications and vision for hands-on evaluation of the Oracle9i Database and its security features," added Maimone. "The tight feedback loop enabled the Oracle team to quickly assess new features and rapidly advise AFRL on their benefits to JBI and C2ISR."

"This effort allowed us to get in on the ground floor six months before commercial release and assist Oracle in refining their security products in order to help meet JBI technical challenges," said Thomas A. Clark, program manager of the effort in the directorate's JBI Office. "We have found a lot of COTS products are not really addressing security issues to the extent that Oracle has in the past and continues to do. This effort allowed us to evaluate a next-generation commercial product and influence its applicability to JBI."

-- 30 --

CONTACTS: AFRL: Francis L. Crumb, (315) 330-3053; E-Mail: crumbf@rl.af.mil;